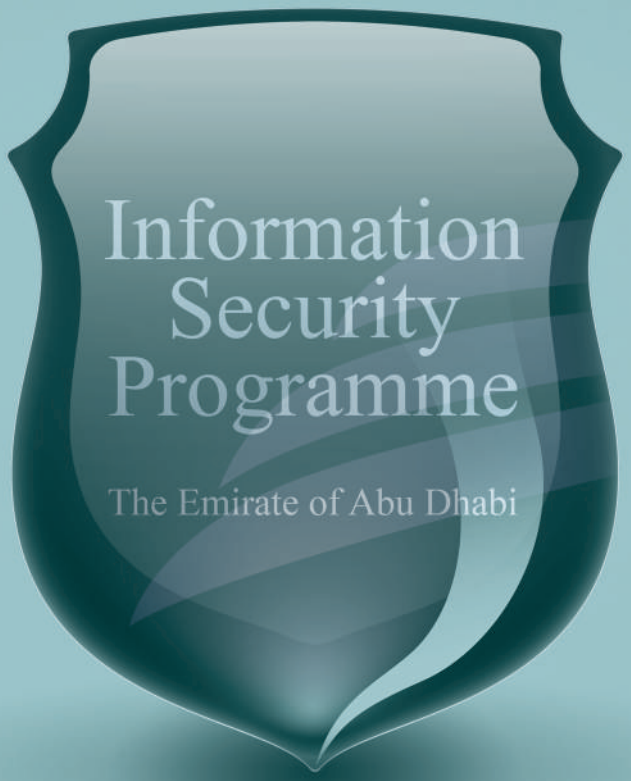
مركز أبوظبي للأنظمة الإلكترونية والمعلومات
Abu Dhabi Systems & Information Centre



INFORMATION SECURITY POLICIES & PROCEDURES

GUIDE

Version 1.0

أبوظبي
abudhabi

GUIDE

INFORMATION SECURITY POLICIES & PROCEDURES

DOCUMENT CONFIGURATION CONTROL

VERSION	RELEASE DATE	SUMMARY OF CHANGES	RELEASE APPROVAL
Version 1.0	15 March 2009	Initial Release	ADSIC, Information Security Team

Document Location

- Abu Dhabi Portal (electronic copy)
- ADSIC Portal and Office (electronic copy and hard copy)

Questions or Comments

Any questions or comments regarding this document should be directed to:
support@adsic.abudhabi.ae

1. Contents

1. INTRODUCTION

1.1 OVERVIEW

The Abu Dhabi Government requires all of its entities to have a Risk Management process in place to manage the information security risks associated with processing Government information. An essential part of Risk Management is a set of policies and procedures that will regulate usage of the Abu Dhabi Government Entity's (henceforth referred to as an ADGE or entity) services and their information system. This *Abu Dhabi Information Security Policies and Procedures Guide* presents a practical starting point for developing and maintaining the full set of information security policies and procedures—the Policies and Procedures Handbook—that each entity must have.

While this Guide provides the overall approach, it is important to realise that each ADGE is different in terms of size, issue complexity, and the deployment of its services. Therefore, the information security policies and procedures within this Guide must be tailored to fit the unique requirements of each ADGE. The Guide examines the rudiments to be considered when developing and maintaining these policies, and presents a design for a suite of information security policies and procedures and their accompanying development and maintenance process.

Information security policies and procedures are a key element of any Risk Management process, as they define the rules for all stakeholders to follow. They help form a consensus regarding best practices that all employees should follow, reducing the risks inherent to information systems use. Well-defined, well-enforced policies will transform employees into active supporters of information security and stakeholders in securing the information assets of the ADGE. These policies define the ADGE's attitude towards information, and announce internally and externally that the information is an asset, property of the ADGE, and is to be protected from unauthorised access, modification, disclosure, and destruction.

Other advantages to having policies and procedures include:

i. Establishing a "paper trail" to assist in future reviews
ii. Demonstrating the ADGE's commitment to information security
iii. Providing a benchmark for measuring progress
iv. Helping to increase consistency
v. Providing support for the Chief Information Security Officer (CISO)

In general, policies and procedures are intended to:

i. Protect people and information
ii. Set the rules for expected behaviour by users, systems administrators, management, and security personnel
iii. Authorise security personnel to monitor, probe, and investigate
iv. Define and authorise the consequences of violations
v. Define the ADGE's baseline stance on security
vi. Help minimise risk
vii. Help track compliance with regulations and legislation
viii. Drive change towards best practices

A key consideration when drafting policies and procedures is the careful balance between functional controls vs. management controls. Not all policies can be implemented solely through functional means. Likewise, management controls are often insufficient on their own and must be supported by technological configurations (i.e., functional controls) to enhance compliance.

To accomplish their objectives, policies and procedures must be workable, realistic, and useful. Staff will be tempted to bypass policies that are overreaching or overly restrictive. Communication with all involved parties—from senior management to staff whose daily work is directly affected—is important to obtain their support. In addition, information security policies should be in line with other, existing policies within the ADGE and should match the culture, attitude, and expectations of the workforce.

Having policies and procedures in place that are useful for employees and management alike will contribute greatly towards their successful implementation. High-quality direction will facilitate daily work routines by providing structure and best practices, and senior management will benefit from the enhanced legal compliance and drive for improvement that results.

1.2 SCOPE

The functional scope of the *Abu Dhabi Information Security Policies and Procedures Guide* centres on information security. By looking beyond the traditional focus of information technology, this ensures that sensitive Government information is protected throughout its lifecycle, not just in the systems where data is processed.

The Abu Dhabi Government fully recognises the importance of developing such a programme in coordination and integration with the related assurance disciplines of physical security, personnel security, business continuity, and cross-functional risk management, and the importance of directing the programme to assure Government missions rather than simply implementing security controls. Each of these related assurance disciplines are included within the programme and contain specific activities to ensure integration under a mission assurance umbrella.

1.3 APPLICABILITY

The *Abu Dhabi Information Security Policies and Procedures Guide* applies to Abu Dhabi Government personnel, contractors, and third party organisations and individuals. It covers all information and information technology assets to include hardware, software, media, facilities, data, and electronically stored information that may be owned, leased, or otherwise in the possession, custody, or control of the Abu Dhabi Government.

1.4 COMPLIANCE AND ENFORCEMENT

Per the Abu Dhabi Information Security Policy, compliance with the Risk Management process is mandatory, and information security policies and procedures play key roles in this process. The implementation of security controls across the Abu Dhabi Government can only be fully effective when all stakeholders operate in a consistent manner.

Personnel and ADGEs found to be non-compliant with the Risk Management process risk having their access to information systems and data revoked, and may be subject to disciplinary actions and legal prosecution as supported by existing laws and policies of the United Arab Emirates (UAE) and Abu Dhabi (e.g., the UAE Cyber Laws). Services that fail to comply with the Risk Management process may not be allowed to process Government information.

Enforcement and monitoring of these standards is the shared responsibility of ADSIC, each Government entity's Chief Information Security Officer (CISO), and the Abu Dhabi Audit Authority.

1.5 DOCUMENT LAYOUT

The Abu Dhabi Information Security Policies and Procedures Guide will provide readers with the information and tools needed to develop and maintain a full set of information security policies and procedures.

- **Section 1** provides the overview, background, and purpose of the Guide, and answers the question, "Why develop an entity-specific Information Security Policies and Procedures Handbook?"
- **Section 2** provides answers to frequently asked questions about entity-specific Information Security Policies and Procedures Handbook and some of their key components
- **Section 3** provides a step-by-step guide to developing an entity-specific Information Security Policy and Procedures Handbook
- **Section 4** provides a draft outline for the initial paragraphs of the Policies and Procedures Handbook
- **Section 5** provides draft policies to be used by entities
- **Sections 6** through 17 provide instructions on how to write specific procedures for selected topics

2. FREQUENTLY ASKED QUESTIONS

2.1 WHAT IS THE DIFFERENCE BETWEEN POLICIES AND PROCEDURES?

Policies and procedures both prescribe how to manage and operate the service and its supporting systems. They are closely intertwined, and a well-crafted set of these documents will provide full guidance to the ADGE, as illustrated in Figure 1.

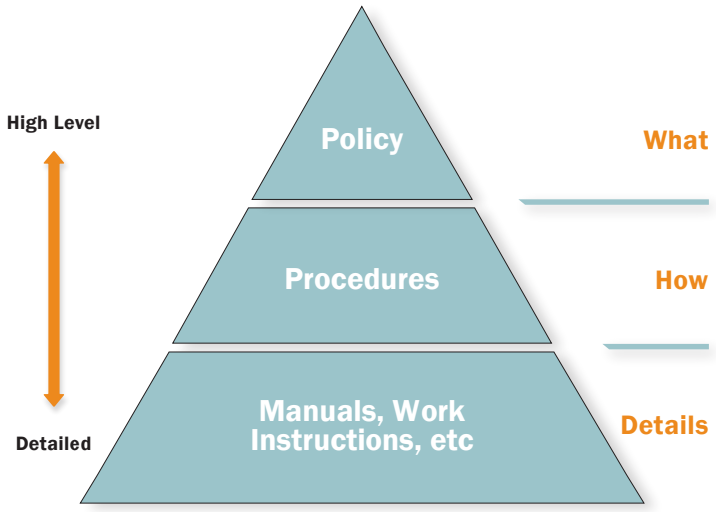


Figure 1: Relationship Between Policies, Procedures, and Other Documents

The first four chapters of this Guide focus on the "Why" question and provides motivation and reasons for setting up a set of policies and procedures tailored for each individual ADGE. It is recommended that similar motivations be included in the Policies and Procedures Handbook that each ADGE is also required to develop.

Policies are formal, brief, and high-level statements or plans that embrace the ADGE's general goals, objectives, and acceptable standards for a specified subject area. They state required actions, often include references to control standards, and answer the question of "What should be done".

Policy attributes include:

i. Required compliance (mandatory)

ii. Disciplinary actions resulting from failure to comply

iii. Focus on desired results rather than means of implementation

iv. Further definition through standards and guidelines

Procedures are mandatory actions or rules designed to support and conform to a policy. They consist of a series of steps to accomplish an end goal, and focus on answering the question of "How" something should be done. The objective of a procedure is to make policies more meaningful and effective—which is achieved by including one or more specifications for hardware, software, or behaviour.

Procedures share importance with policies, as the two complement each other. For example, a backup policy might prescribe that all crucial data be backed up daily. The backup procedure will complement this through detailed instructions of how to execute the backup—what data is crucial; whether to use tape, optical, or network media; how to label backup media; specific transportation and storage requirements; etc.

From this example, it is clear that a single policy can be connected to multiple procedures—one procedure for each system that needs to be backed up. If further detail is required, it is often recommended that the procedures be supplemented with user guides, manuals, and work instructions as shown in the lowest layer of the pyramid in Figure 1.

2.2 HOW DO THESE POLICIES AND PROCEDURES RELATE TO THE INFORMATION SECURITY PLANS FOR EACH SERVICE?

The Information Security Plan for each service describes in detail what controls are in place, or are planned to be implemented, to protect the information processed and stored by that service and its supporting systems. Many of those controls are, or should be, captured in and supported by policies and procedures. Formalised, written, and approved policies and procedures greatly help in securing a service because they enforce standardised, repeatable best practices for system use, operation, monitoring, and maintenance. While a lack of policies and procedures does not necessarily mean that underlying processes are not being executed safely, it also does not contribute to reducing potential risks to an acceptable level.

2.3 SHOULD SEPARATE POLICIES AND PROCEDURES BE DEVELOPED FOR EACH INDIVIDUAL SERVICE WITHIN AN ADGE?

Most, if not all, ADGEs have multiple services with supporting systems, which begs the question of "How specific policies and procedures should be"—can they be shared by the various services within the entity, or be developed individually for each service?

The short answer to this question is "no" for policies and "yes" for procedures, due to several important nuances. Since policies are more generic in nature, they can be applied across services relatively easily. A policy that is applicable to only one service should be evaluated, as it might be rewritten as a procedure instead.

For procedures, the situation is slightly more complex and depends on the ADGE's organisational structure, as shown in the following illustration:

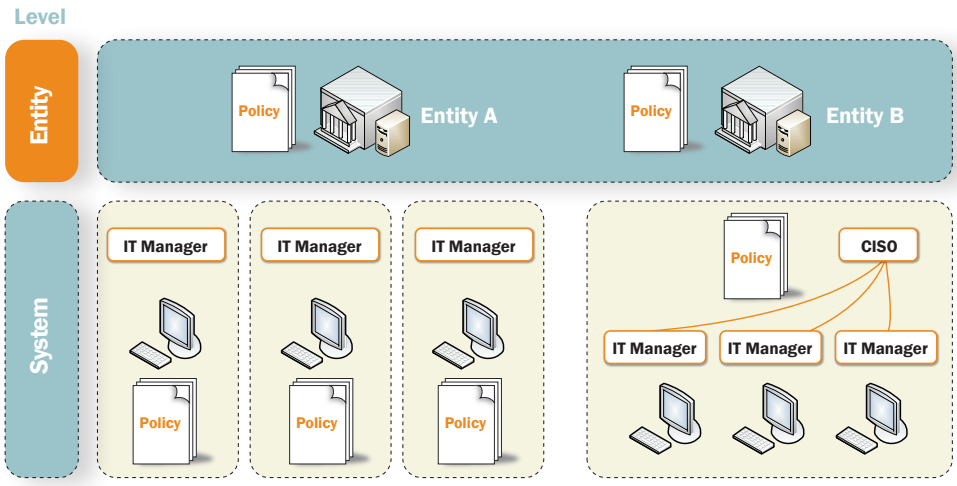


Figure 2: Comparison of the Location of Policies and Procedures

In Figure 2, entity A does not have a dedicated CISO, while entity B has established this function. This allows entity B to coordinate the development of procedures across its various services.

Note that while the presence of a CISO in entity B facilitates the sharing of procedures across its services and reduces the efforts involved in their development and maintenance, nothing would

prevent the information technology (IT) managers at entity A from collaborating with each other. By sharing their procedures, they too could reduce the time needed for development and maintenance.

Not all procedures, however, can be shared across different services. Some procedures track specifically with a certain service and/or system, while in other cases multiple services might differ from each other too much for a common procedure to apply. In these situations, ADGEs are required to develop procedures that are tailored to an individual service.

2.4 SHOULD EACH ADGE FOLLOW THIS GUIDE EXACTLY?

As per the Abu Dhabi Risk Management process, ADGEs are required to develop and maintain their own information security policies and procedures. This Guide helps each ADGE set up a handbook of information security policies and procedures that contains a fully developed set of all policies needed to comply with the Information Security Standards of the Abu Dhabi Risk Management process. It also provides outlines for the major procedures all ADGEs are expected to have.

ADGEs without formalised, documented policies and procedures could be ordered to cease operation of their services on the grounds that they could fail the third and fourth phases (i.e., Security Testing and Evaluation, Certification and Accreditation) of the Risk Management process. Following this Guide will greatly increase the likelihood of an ADGE having its services accredited—but what ultimately matters is for the entity to have policies and procedures in place. ADGEs desiring to follow their own methodology to create a handbook are free to do so provided the end result is compliant with the *Abu Dhabi Information Security Standards*.

As mentioned in Section 1.1, Overview, each ADGE is expected to tailor the policies and outlined procedures in this Guide to its specific circumstances. While the Guide provides a solid starting point, a verbatim copy-and-paste will not produce a handbook that can be accurately applied to the ADGE's own needs.

2.5 HOW SHOULD THE POLICIES AND PROCEDURES BE ORGANISED?

The recommended way for ADGEs to organise their policies and procedures is included in this Guide, and is in line with the control families that form the basis of the *Abu Dhabi Information Security Standards.*

CONTROL FAMILY	ACRONYM	TYPE
Strategy and Planning	SP	Management
Policy and Standards	PS	Management
Risk Management	RM	Management
Awareness and Training	AT	Management
Communications and Outreach	CO	Management
Performance Management	PM	Management
Asset Management	AM	Functional
Human Resources Security	HR	Functional
Physical and Environment Security	PE	Functional

CONTROL FAMILY	ACRONYM	TYPE
Communications and Operations Management	CM	Functional
Identity and Access Management	IA	Functional
Information Systems Acquisition, Development and Maintenance	IS	Functional
Incident Management	IM	Functional
Business Continuity Management	BC	Functional

Table 1: List of Control Families

Applying the organisational structure shown above ensures that an ADGE's handbook will be consistent with the overall Abu Dhabi Risk Management process and will facilitate the evaluation of policies and procedures that takes place during the Security Testing and Evaluation phase.

ADGEs that prefer to deviate from this structure should include a translation table in their handbook that maps their structure to the directory in Table 1.

An important distinction between the types of policies and procedures being offered should be made according to the audience. While members of an IT department would typically want the full set of policies, regular end users should be offered a set that focuses on their role in information security, written in easy-to-understand, non-technical language, that contains only material relevant to their needs. An example of this is found in Chapter 16, Outline Acceptable Use Policy.

2.6 WHAT IS THE BEST SEQUENCING TO THE DEVELOPMENT OF THESE POLICIES AND PROCEDURES?

When creating an original document, a good approach is to develop the acceptable use policy first. This policy affects all users, and has high visibility and impact. Distributing and requiring all employees to sign a copy of the acceptable use policy for compliance purposes will call attention to the ADGE's emerging policies and procedures effort.

The next step could be to develop a user password policy, since this also affects end users directly. Any subsequent policies and procedures would then reach an audience already familiar with the concept of having to comply with information security standards.

Some policies and procedures can be developed in parallel with others, and often by different teams. The development of policies related to a single service (e.g., related to physical security) can be driven by subject matter experts. This will speed up the development process and help sustain momentum. Procedures are typically developed once their guiding policies are in place.

2.7 WHAT IF EMPLOYEES DO NOT LIKE THE NEW POLICIES AND PROCEDURES?

The truth behind the common maxim that "people fear change" is demonstrated frequently in the roll-out of new policies and procedures. Many employees are afraid that new directives will change a way of work to which they have grown accustomed. They may also feel limited by the boundaries set by the new guidelines. Also, management might fear the additional costs of becoming compliant with the new requirements being forced upon them.

These concerns should be taken seriously by the development team, as users often have rational reasons for their fears. Policies and procedures will change the way they work, will limit them, and a financial outlay will be required to become compliant. The very point behind drawing up new policies and procedures is to change the way that people work.

Rather than denying the validity of these fears, the development team should address them and explain the reasons for having policies and procedures in place. Section 1.1 of this Guide lists common benefits and objectives—and makes clear that while there might be initial growing pains, the end result is worth it. Also, despite the initial increase in costs, many studies have shown that compliance with its policies and procedures is actually a money-saver for the organisation: as the ADGE moves towards best practices, its processes are refined, resulting in cost reductions.

A good way to obtain buy-in is for the development team to involve end users in the process by clearly communicating what is going to happen; how and when end users can contribute and influence the outcome; and how compliance with policies and procedures can benefit each individual. This provides ample room for participation, but it is important to stand firm on the overall purpose—that policies and procedures are going to be developed, preferably with, but if necessary without, the wholehearted support of each and every employee.

3. HANDBOOK DEVELOPMENT STEPS

The Policies and Procedures Handbook development process is divided into seven steps that will be described in this section:

Figure 3: Handbook Development Steps

3.1 OBTAIN SENIOR MANAGEMENT BUY-IN

Prior to developing policies and procedures, it is essential to have senior management approve of the process and resources that will be required. Setting up this type of framework is a serious endeavour that involves substantial amounts of time and resources. Both the writers and the support staff that will provide input throughout the development process must be accessible.

To determine the necessary resources, the project manager—typically the CISO—must clearly outline the scope of the handbook and the order in which the policies and procedures will be developed. It is recommended to treat the handbook's development as a stand-alone project and apply the relevant project management standards, which are outside the scope of this Guide.

Senior management buy-in will ensure that all required resources will be present and willing to cooperate throughout the development process. Requiring senior management to commit themselves to the establishment of information security policies and procedures will also guarantee that they are aware of the importance and scope of the process. Having this approval will facilitate the allocation of resources for each individual policy/procedure development cycle. A final benefit of senior buy-in is that it will signal to all stakeholders the importance being attached to information security within the ADGE.

It is usually a good idea to have senior management decide on a grace period after which a newly implemented policy or procedure will become effective. Announcing this grace period up front will reduce potential anxiety among those who must comply by providing relevant stakeholders with sufficient time to review and implement any project, processes, or internal communications needed to ensure compliance.

3.2 ALLOCATE RESOURCES

Allocation of the proper resources is an important task in ensuring the timely delivery of high quality policies and procedures. The development process should not start until all required resources have been secured for the necessary timeframe. When it is necessary to outsource a portion of the work to a third party, clear agreements should be reached regarding availability of this resource as well.

The core development team should typically consist of those who will own and enforce the policy or procedure upon its completion. While the team's exact makeup depends on the policy or procedure to be developed, a workable approach would be to have the following groups involved in the development process:

Chief Information Security Officer (CISO)	The CISO sets up a team which should be assigned overall responsibility for developing the Handbook. Overall control may be given to one person, with others in a supporting role. This team will guide each policy/procedure document through development and revision, and should subsequently be available to answer questions and consult.
Technical Writer(s)	The ADGE may already have a technical writer on staff that can assist in writing security policies/procedures. Even if this individual is not able to take primary responsibility for the project, an in-house writer can be a valuable resource for planning the project, determining an appropriate document style and formatting structure, and editing/proofreading drafts.
Technical Personnel	In addition to security team staff, the ADGE may need to call upon the expertise of staff with specific security and/or technical knowledge in the area related to a specific policy/procedure. These individuals should be familiar with the day-to-day use of the technology or system for which the policy/procedure is being developed, and they can provide input on what is good security and what is feasible within the ADGE.
Legal Department	The ADGE's Legal Department should review the policy/procedure documents once they are complete. This group will be able to provide advice on relevant legislation that requires certain types of information to be protected in specific ways, as well as on other legal issues. The Legal Department should also assist with the development process through notifying and explaining forthcoming legislative requirements to the team.
Human Resources Department	The Human Resources Department may need to review and/or approve the policy/procedure depending on how it relates to existing ADGE guidance. Where it touches on topics covered by existing Human Resources guidelines (e.g., e-mail usage, physical security), Human Resources must make sure that both sets of regulations are in accordance.
Audit and Compliance	Because the ADGE's Internal Audit Department is likely to be involved in monitoring ADGE-wide compliance with the policy/procedure once it is in force, it is useful if this group is involved in the development and review processes to ensure that it is enforceable in terms of audit activities and current best practices. Any additional ADGE compliance groups should also be consulted.
User Groups	It can be useful to work with users during the revision of the policy/procedure documents to determine how successful the current policy/procedure is. This can help determine how the policy/procedure may need to be changed to make it more useable for the target audiences. While issues such as document style, layout, and wording may seem minor in comparison with what they contain, documents that are off-putting or hard to understand may not be fully read or understood, needlessly risking security compromise.

Review Team	Once the policy/procedure has been drafted, a thorough review is essential to ensure consistent quality. It is usually a good idea to appoint a few dedicated reviewers to evaluate and comment on the draft, who can draw upon experts and other stakeholders as necessary. (See Section 3.4 for additional details on the reviewing process.)

3.3 DEVELOP DRAFT/REVIEW EXISTING POLICY

When beginning the development process for a new policy/procedure, it is worthwhile to check if related policies/procedures already exist. Such guidelines can serve as a good starting point, and could possibly be incorporated into the new policy/procedure. Depending on the existing material's quality and relevance, a simple review with minor adjustments and updates might be sufficient.

If no policy/procedure currently exists, or is of insufficient quality, the ADGE must develop something new. Useful resources for this can include subject matter experts, the Internet (provided the Web sites referred to are treated with professional scepticism), this Guide, journals, books, and white papers. Other related documents to consider prior to writing a new policy/procedure include job descriptions, guidelines, instructions, user guides, manuals, etc. as they often provide insight into available management and technical controls and methods.

Policies (and to a lesser extent procedures) should be designed to remain reasonably stable. Any instance of policies and procedures becoming quickly outdated should be taken seriously, as this makes them less relevant and therefore more likely to be ignored. Outdated material could result from a review cycle that has taken too much time, or from language that is too specific. Policies, in particular, should be generic without being vague.

The actual language of the policy/procedure requires a delicate sense of balance. If it is too lenient, it will reduce the impact of the policy/procedure; if it is too rigid, the audience might create alternative ways to bypass the intended requirements. It is also recommended that an exception process be established. Rather than including all possible exceptions in the policy/procedure document and weakening it, a separate process should be defined to review and grant stakeholder requests for situations to be treated exceptionally.

Other points to consider while drafting a policy/procedure include:

i. Making use of the ADGE's style guide, if one exists. Applying the style guide will ensure the policy/procedure documents are in line with other entity documents, and enhance consistency across different policies/procedures. Consider developing a style guide if there is not one already.

ii. Ensuring consistency of style. The CISO should make basic decisions as to style of the policies/procedures (e.g., active voice vs. passive voice) before starting work on the document.

iii. Making the wording of directions as specific as possible (e.g., "backups must be made every week" rather than "backups must be made periodically").

iv. Avoiding the use of extremes such as "always" or "never." While these may sound clear and precise, such words often introduce gradients of compliance and will challenge the audience to come up with exceptions—which will serve to weaken the policies/procedures.

v. Making policies/procedures concise and to the point. Easy-to-understand language is preferred over difficult, long-winded sentences, because material that no one understands is likely to be ignored.

vi. Ensuring that policies/procedures do not include the personal names of employees—they should refer to job functions, titles, and positions to ensure they remain applicable following staffing changes.

vii. Writing policies/procedures that are appropriate for their respective audiences—for example, it is not realistic for general employees to be expected to read and understand documents intended for technical security specialists. A more appropriate document would be a tailored Acceptable Use Policy for end users, as outlined in Chapter 16. It is also not recommended for technical security specialists to receive the condensed security documents intended for basic end users.

3.4 REVIEW WITH STAKEHOLDERS

A thorough review of the draft policy/procedure is important to ensure that it is in line with the ADGE's mission statement, as well as to detect factual errors, grammatical mistakes, style inconsistencies, and layout irregularities. Initial rounds of review usually take place within the team set up by the CISO, and are later expanded to include other supporting teams. It is also a good idea to ask an outsider (i.e., outsider to the CISO's team, yet employee within the entity) to review the document. Not only might a fresh set of eyes detect previously undiscovered errors, but it also provides a good opportunity to test whether the policy/procedure can be understood by someone not overly familiar with the topic at hand.

A common problem is that reviewers do not seem to provide useful, in-depth feedback. Best-case, this can be caused by policies/procedures that are of excellent quality and require few comments. But more often, limited feedback is the result of either a lack of true understanding or sufficient time for the review process. The first case can be addressed by providing feedback training and other forms of instruction that address the purpose of the policy or procedure, and what is expected of the reviewers. A lack of time can be solved by providing the policies and procedures to reviewers in a way that ensures that they have appropriate time to perform their assessments.

Another way of increasing the quality of feedback is to organise group sessions with all reviewers. This can often generate discussions with valuable results.

At times, however, a review cycle can drag out. This can be caused by an overly large review team, reviewers who avoid taking responsibility, or individuals who feel they do not have sufficient responsibility for providing feedback. The core review team should consist of two, three, or four people, augmented by other reviewers depending on the nature and scope of the material being assessed. Using more than eight reviewers will make the process unduly weighty while not enhancing the quality of the feedback itself. Reviewers who shy away from taking responsibility should be told that drafting policies and procedures often depends on compromise. Also, it is recommended that persons selected as reviewers are employees who can make decisions without overstepping their responsibilities.

3.5 OBTAIN SENIOR MANAGEMENT SIGN-OFF

After a draft policy/procedure has been properly reviewed, it must be submitted to senior management for approval. This level of approval will provide the needed authority to augment the chances of its successful implementation within the ADGE.

While this refers to individual policies and procedures, the Handbook will also need to be formally approved. It is recommended to let the highest function within the ADGE write a paragraph stating his/her commitment to the Handbook and making clear that all employees should abide by the material it contains. This paragraph is most effective if accompanied by a formal signature of endorsement. A sample text is included in Section 4.1.

3.6 PUBLISH AND COMMUNICATE HANDBOOK

To be followed, a Handbook must first be read by its intended audience. This makes effective publication and communication very important. Publication is relatively simple and can be achieved by placing the new or updated Handbook on the ADGE's intranet. This approach is recommended to enable employees to download, save, and print the policies and procedures that the Handbook contains.

Effective communication, however, is more of a challenge. To be sure that all employees have read the ADGE's Handbook, it is recommended that all employees be required to sign a statement affirming that they are aware of, and will keep up to date with, all policies and procedures listed in the Handbook that are applicable to their job functions.

It is not realistic to expect all employees, contractors, and third party associates of the ADGE to read the complete Handbook, especially since certain sections are rather technical in nature. A workable solution is to create an Acceptable Use Policy that focuses solely on the responsibilities of end users, which they would be required to sign prior to being given access to the ADGE's information systems. A detailed sample text for this is found in Chapter 16.

Other, less formal approaches include making policy/procedure awareness part of the ADGE's training programme, and sending out e-mails informing staff about changes to the Handbook.

During the first stage of implementing new policies and procedures, enthusiasm among end users to adhere to them is often yet to be established. However, this should not cause immediate concern. Taking policies and procedures seriously usually comes with time and an increasing number of policies and procedures, supported and promoted by a combination of management backing and a good awareness and communication campaign. The result of a well-thought out campaign should be that stakeholders increasingly realise that policies and procedures can be used to leverage change and drive existing processes towards best practices.

3.7 MAINTAIN HANDBOOK

Maintenance of the Handbook should take place frequently—at least once every year. This will allow the ADGE to evaluate its policies/procedures by obtaining feedback from employees who must adhere to them, and from the Internal Audit Department responsible for monitoring their compliance. Significant compliance issues could indicate that the policy/procedure is not enforceable, whereas the targeted audience could provide feedback on developments such as new legislation, changed best practices, an updated ADGE mission statement, etc. These lessons learned must be incorporated in the updated version to strengthen the policies/procedures.

The maintenance cycle is similar to the process mentioned in the earlier steps, as shown in Figure 4. The most significant difference is the shorter time span for rewriting and reviewing updates.

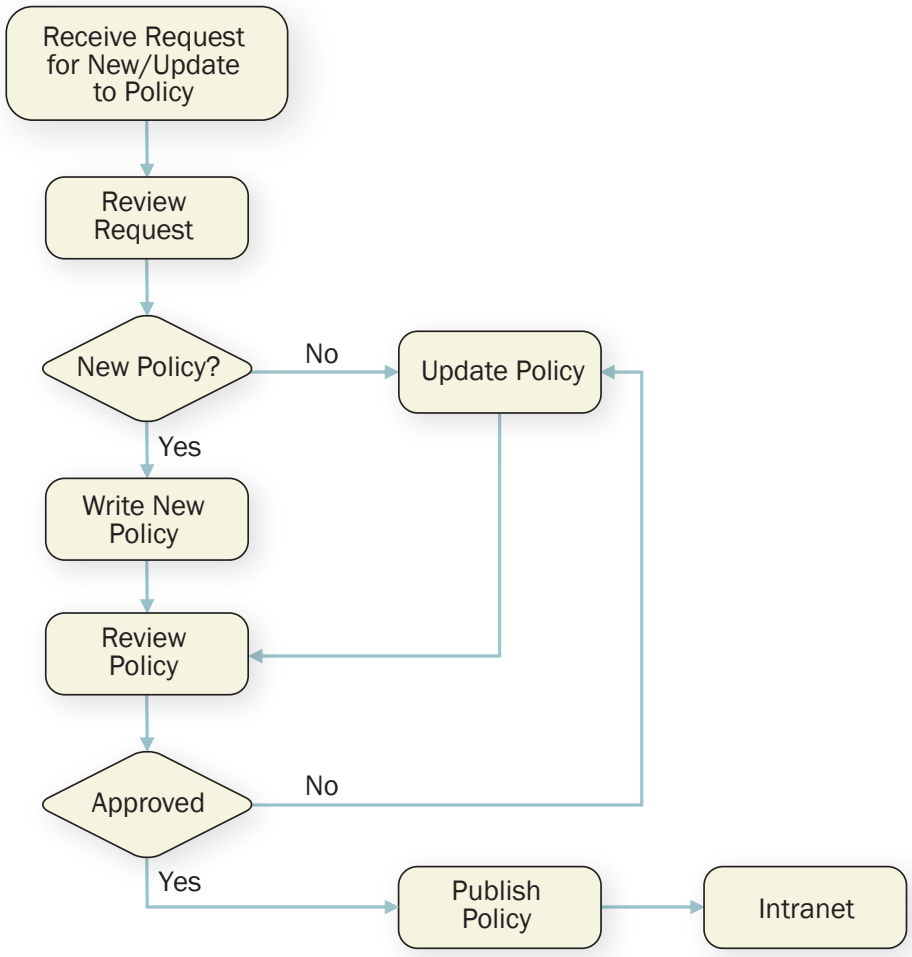


Figure 4: Informatiion Security Policy Lifecycle

4. SAMPLE HANDBOOK

This chapter provides a sample Information Security Policies and Procedures Handbook for entities. While every care has been taken to be complete and correct, it is impossible to write a generic handbook that applies to every entity. As such, entities are recommended to adapt the content of this sample handbook to their specific situation.

4.1 MANAGEMENT ENDORSEMENT

MANAGEMENT ENDORSEMENT

[NAME OF HIGHEST RANKING ENTITY OFFICIAL]
[TITLE OF HIGHEST RANKING ENTITY OFFICIAL]

The purpose of this Policies and Procedures Handbook is to protect the ***[ENTITY]***'s information assets from all threats.

The general management of the ***[ENTITY]*** is committed to comply with this Handbook and strongly support its implementation.

I hereby request that all staff read the Handbook comprehensively and comply with its supportive detailed policies and procedures.

Breaches of information security, be they internal or external, deliberate or accidental, must be reported to, documented and investigated by the Chief Information Security Officer (CISO).

All managers of the ***[ENTITY]*** are directly responsible for implementing this handbook and its supported policies and procedures within their respective areas. It is expected from all staff members, at all levels, to adhere to the Policies and Procedures Handbook.

[NAME OF HIGHEST RANKING ENTITY OFFICIAL] of the ***[ENTITY]*** has approved this Policies and Procedures Handbook.

Signed: Date:

4.2 OVERVIEW

The objectives of the ***[ENTITY]***'s policies and procedures are to:

i. Protect people and information
ii. Set the rules for expected behaviour by users, System Administrators, management, and security personnel
iii. Authorise security personnel to monitor, probe, and investigate
iv. Define and authorise the consequences of violations
v. Define the entity consensus baseline stance on security
vi. Help minimise risk
vii. Help track compliance with regulations and legislation
viii. Drive change towards best practices

4.3 SCOPE

The policies and procedures in this document are intended to cover all aspects of information security insofar as they are under the direct or indirect control of the ***[ENTITY]***.

4.4 APPLICABILITY

The policies and procedures contained within this handbook apply to all ***[ENTITY]*** employees, including part-time staff, trainees, contractors, and other third party associates.

Threats to the *[ENTITY]* covered by this policy pertain to the following assets:

1. Information held and processed on behalf of clients or for internal purposes, whether paper-based or computerised
2. Services, their supporting systems, and other equipment
3. The ***[ENTITY]*** employees
4. The ***[ENTITY]*** buildings and premises

This policy must be reviewed on a yearly basis and updated as necessary.

4.5 COMPLIANCE AND ENFORCEMENT

Compliance with the policies and procedures contained in this handbook is mandatory. All ***[ENTITY]*** personnel, contractors, and third party organisations and individuals must comply with the roles, responsibilities, and security policies set forth in this document to ensure the confidentiality, integrity, and availability of all Government information. This includes all information and information technology assets, including hardware, software, media, facilities, data, and information stored electronically, that may be owned, leased, or otherwise in the possession, custody, or control of the ***[ENTITY]***.

Personnel and entities found to be non-compliant with this Policies and Procedures Handbook may have their access to information systems and data revoked, and may be subject to criminal disciplinary actions as supported by existing laws and policies of the United Arab Emirates (UAE) and the Emirate of Abu Dhabi. Services that fail to comply with this policy may not be allowed to process Government information.

Enforcement and monitoring of this policy is a shared responsibility of the ***[ENTITY]***'s CISO and the Abu Dhabi Audit Authority. Specific roles and responsibilities are further delineated in the Roles and Responsibilities section of this document.

4.6 DOCUMENT LAYOUT

This document has four main sections.

- Section 1 (that is Section 4 in this Guide) provides the overview, background, and purpose of this document.
- Section 2 (that is Section 5 in this Guide) contains the policies of the ***[ENTITY]***, grouped into 14 areas in line with Abu Dhabi's Information Security Standards. For each area, a brief overview is given, followed by the detailed policies. These policies are mandatory statements that all employees of the ***[ENTITY]*** must follow.

The 14 areas around which the policies are grouped include:

	CONTROL FAMILY	ACRONYM	TYPE
1	Strategy and Planning	SP	Management
2	Policy and Standards	PS	Management
3	Risk Management	RM	Management
4	Awareness and Training	AT	Management
5	Communications and Outreach	CO	Management
6	Performance Management	PM	Management
7	Asset Management	AM	Functional
8	Human Resources Security	HR	Functional
9	Physical and Environment Security	PE	Functional
10	Communications and Operations Management	CM	Functional
11	Identity and Access Management	IA	Functional
12	Information Systems Acquisition, Development and Maintenance	IS	Functional
13	Incident Management	IM	Functional
14	Business Continuity Management	BC	Functional

Table 2: List of Control Families

- Section 3 (that is Section 6 in this Guide) provides detailed roles and responsibilities as they are referred to in the policies and procedures contained within this document.
- Section 4 (that is Section 17 in this Guide) provides a glossary of terms used throughout this document.
- Sections 5 – 13 (those are Sections 7 - 15 in this Guide) contain outlines for various procedures that undergird the policies for the ***[ENTITY]***, and are intended to provide additional guidance and practical steps to implement many important procedures.

5. SAMPLE POLICIES

Overview:

The objective of Strategy and Planning is to provide information security governance for the Entity. This primarily involves creating the internal oversight and management needed to consistently and adequately implement information security, and establish information security plans for individual systems.

5.1 STRATEGY AND PLANNING

5.1.1 INFORMATION SECURITY PLANNING POLICY (SP 1.2.3, SP 1.3.1, SP 1.3.2, SP 1.3.3)[1]

a) A position of a Chief Information Security Officer (CISO) must be established and filled by a suitably competent individual, who will be responsible for leading and managing the ***[ENTITY]*** Information Security Programme.

b) The scope and boundaries of each service must be defined—specifically in terms of the characteristics of the business it supports, the entity, its location, its assets (including asset owners), and its technologies, as well as the details of/justification for any identified exclusions from the scope of control.

c) A risk profile must be created for each service that should include identification and evaluation of risks to the system's assets. Identification of such risks must include threats to assets, vulnerabilities that may be exploited by the threats, and the possible impact that loss of confidentiality, integrity, and availability may have on the assets. In addition, the risk profile analysis for each service must include business impacts due to system security failures, likelihood of security failures, definition of acceptable risk, and estimated level of risk.

d) Appropriate controls must be selected and implemented to ensure that risks are either mitigated or reduced to an acceptable level. In addition, appropriate controls must be selected and implemented in full consideration of all applicable legal legislation, compliance with intellectual property rights, protection of organisational records, protection of the privacy of personal information, and to prevent misuse by information processing facilities.

[1] *References in brackets refer to the corresponding control standards in the Information Security Standards document.*

5.2 POLICIES AND STANDARDS

Overview:

The objective of Policies and Standards is to define the requirements and responsibilities that the entity must follow within each of the necessary policy areas. These policies must be developed to make them consistent with the official Abu Dhabi Information Security Policy and Information Security Standards.

5.2.1 INFORMATION SECURITY POLICY (PS 2.1.2, PS 2.2.2)

a) A capstone information security policy document must be established to govern the information security efforts of the ***[ENTITY]***. This document must set forth all applicable policies, security roles/responsibilities, and supporting information security procedures for the entity. It must be reviewed on a yearly basis and updated as necessary.

5.3 RISK MANAGEMENT

Overview:

The objective of Risk Management is to empower the entity with a structured and effective approach to managing the uncertainty related to threats and vulnerabilities. This approach follows a sequence of activities that includes conducting a risk assessment, developing strategies to manage known risks, implementing applicable controls to mitigate risks, verification and validation of control implementation, execution of a management process to accept residual risks, and the performance of ongoing risk management.

5.3.1 Risk Management Policy (RM 3.1, RM 3.2, RM 3.3, RM 3.4)

a) A risk assessment must be executed on all services at least once every three years or whenever major changes to the services have occurred. These assessments must be conducted annually for high-risk services. Risk assessments must be conducted in full accordance with the Abu Dhabi Government's established Risk Assessment process.

b) Security Testing and Evaluation (ST&E) of all services must be conducted prior to the systems going live. Services categorised as HIGH must undergo ST&E conducted by an independent party, while services categorised as MODERATE must undergo independent ST&E at the discretion of the CISO. This ST&E must be conduced in full accordance with the Abu Dhabi Government's established Security Testing & Evaluation procedures.

c) All services must go through a Certification and Accreditation (C&A) process prior to going live. Services categorised as HIGH must obtain certification by the Abu Dhabi Government – Information Security Office (ADG-ISO), while services categorised as MODERATE must undergo independent ADG-ISO certification at the discretion of the CISO. This C&A must be conducted in accordance with the Abu Dhabi Government's established Certification & Accreditation procedures.

d) Ongoing monitoring and mitigation of risks against services must be conducted.

5.4 AWARENESS AND TRAINING

Overview:

The objective of Awareness and Training is to provide a formal approach to educating the employees of the entity regarding their roles and responsibilities with respect to information security.

5.4.1 INFORMATION SECURITY AWARENESS AND TRAINING POLICY (AT 4.1, AT 4.2)

a) The Chief Information Security Officer (CISO) must lead an entity-wide security awareness campaign that delivers targeted information security awareness content to all service users and members of management prior to granting users access to the entity's systems.

b) All employees of the ***[ENTITY]***—and third party users, where relevant—must receive appropriate, role-based training and regular updates in organisational policies and procedures. This training must cover security requirements, legal responsibilities, and business controls, as well as instruction in the correct use of information processing facilities (e.g., log-on procedures, use of software packages) before access to information or services is granted.

5.5 COMMUNICATIONS AND OUTREACH

Overview:

The objective of Communications and Outreach is to craft and deliver targeted informational messages and facilitate dialogue with external stakeholders to include industry information sharing and lessons learned.

5.5.1 COMMUNICATIONS AND OUTREACH POLICIES (CO 5.1.1, CO 5.1.2, CO 5.2.1, CO 5.2.2)

a) The Chief Information Security Officer (CISO) must work with the Abu Dhabi Systems & Information Centre (ADSIC) to create and deliver specific internal information security communications aimed at expanding the audience's knowledge of critical information security topic areas. These areas include the Abu Dhabi Government's Information Security Programme and progress against achieving security programme goals.

b) The ***[ENTITY]***'s CISO must work with ADSIC to identify communication requirements to parties outside the organisation, and must work with ADSIC to coordinate with external parties to facilitate the delivery of communication requirements to those groups.

5.6 PERFORMANCE MANAGEMENT

Overview:

The objective of Performance Management is to provide metrics and benchmarks to measure progress and gaps of the Information Security Programme and allow an external audit to validate the intended progress.

5.6.1 PERFORMANCE MANAGEMENT POLICY (PM 6.2.1, PM 6.2.2, PM 6.2.3)

a) The Chief Information Security Officer (CISO) must work with the Abu Dhabi Systems & Information Centre (ADSIC) to develop quantifiable metrics of the ***[ENTITY]***'s Information Security Programme's success. The CISO must also work with ADSIC to gather evidence of the Information Security Programme performance from stakeholders and users, and must work with ADSIC to process and communicate the results of this evidence.

5.7 ASSET MANAGEMENT

Overview:

The objective of Asset Management is to achieve and maintain appropriate protection of organisational assets. This is done by ensuring that every information asset has an owner, the nature and value of each asset is fully understood, and the boundaries of acceptable use are clearly defined for anyone who has access to the information.

5.7.1 ASSET INVENTORY POLICY (AM 7.1.1A, AM 7.1.1C)

a) An inventory of the important assets associated with each service must be drawn up and maintained. Each asset must be clearly identified, and its ownership and security categorisation agreed upon and documented together with its current location (important when attempting to recover from loss or damage). Automated mechanisms must be used to update inventory services labelled as HIGH.

5.7.2 ASSET CATEGORISATION POLICY (AM 7.2.1)

a) Information and outputs from systems must be labelled in terms of their value and criticality to the ***[ENTITY]*** in terms of their confidentiality, integrity and availability requirements. (Additional information is found in the Data Classification Procedure in Chapter 15).

b) Categorisation of assets must be periodically reviewed and adjusted to reflect current status where necessary.

c) Responsibility for defining the categorisation of an item of information for a document, data record, data file, or other form of information media, and for periodically reviewing that categorisation, must remain with the originator or nominated owner of the information.

5.8 HUMAN RESOURCES SECURITY

Overview:

The objective of Human Resources Security is to ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles for which they are considered to reduce the risk of theft, fraud, or facilities misuse.

5.8.1 JOB DESCRIPTION POLICY (HR 8.1.1, HR 8.1.3)

a) Security roles and responsibilities must be documented in job descriptions and elsewhere when appropriate. They must include general responsibilities for implementing or maintaining security policy, as well as specific responsibilities for the protection of particular assets or the execution of particular security processes or activities.

b) Terms and conditions of employment must state the employee's responsibility for information security. Where appropriate, these responsibilities must continue for a defined period following termination of employment. Action to be taken if the employee disregards security requirements must be covered in the terms and conditions. The employee's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation) must also be clarified and included in the terms and conditions. Responsibility for categorisation and management of the employer's data must be included as well. Whenever appropriate, terms and conditions of employment must state that these responsibilities are extended outside the ***[ENTITY]***'s premises and outside normal working hours (e.g., in the case of working from home).

5.8.2 EMPLOYEE SCREENING POLICY (HR 8.1.2)

a) Verification checks on permanent staff must be carried out at the time a position is applied for, in accordance with the Abu Dhabi Police. These must include the following controls: availability of satisfactory character references (e.g., one business and one personal); a check for completeness and accuracy of the applicant's curriculum vitae; confirmation of claimed academic and professional qualifications; an independent identity check that includes a passport or similar document; and a background check on the criminal record of the hire.

b) In the event that the employment, either upon initial appointment or through a promotion, involves the applicant's access to information processing facilities—in particular, involving the handling of sensitive data (e.g., financial or highly confidential information)—the ***[ENTITY]*** must also conduct a credit check on the applicant. For staff holding positions of considerable authority, this check must be repeated periodically.

c) A screening process must be carried out for contractors and temporary staff. When these individuals are obtained via an "agency", the contract must clearly specify the agency's responsibilities for screening and the notification procedures that must be followed if screening is incomplete or if results give cause for doubt or concern.

d) Management must evaluate the supervision required for new and inexperienced staff that have been authorised for access to sensitive systems. Work from all staff must be subject to periodic review and approval procedures by a more senior staff member.

e) Management must be aware that a staff member's personal circumstances can affect his or her work. Personal or financial problems, changes in behaviour or lifestyle, recurring absences, and evidence of stress or depression can lead to fraud, theft, error, or other security implications. This type of information must be handled in accordance with the appropriate legislation.

5.8.3 INFORMATION SECURITY BREACH POLICY (HR 8.2.2)

a) Disciplinary actions may be taken in the event of an employee breach of information security policy and related procedures. Possible actions could range from a formal warning up to dismissal and legal action.

b) The Human Resources Director must take initiative for any disciplinary action after consultation with the Information Security Officer, Information System Head, the head of the department under which the employee resides, and other members of management where necessary.

5.8.4 EXIT POLICY (HR 8.3.1, HR 8.3.2, HR 8.3.3)

a) The following conditions must be met prior to any staff leaving the ***[ENTITY]***, whether voluntarily or involuntarily. All entity assets must be returned, including policy and procedures manuals and technical documentation. Keys, passes, and other access devices must be surrendered. Access identifiers must be deactivated or deleted, and all access authorities must be removed, to revoke access to information systems.

b) Management must ensure that individuals leaving the entity under duress or with ill feelings do not have access to information assets at any time during their period of notice. Escalating the exit procedures to immediately revoke system access is a recommended first step. For additional protection, the individual—particularly if he or she has served in a position of trust—must not be permitted to serve the usual period of notice and must be escorted from the premises.

c) Similar procedures must be applied to personnel who have temporarily or permanently changed positions within the entity, particularly if moving from a sensitive position to a less sensitive one.

5.9 PHYSICAL AND ENVIRONMENT SECURITY

Overview:

The objective of Physical and Environmental Security is to provide standards for the protection of personnel, hardware, programmes, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

5.9.1 PHYSICAL SECURITY POLICY (PE 9.1)

a) The security perimeter must be clearly documented.

b) The perimeter of a building or site containing the ***[ENTITY]***'s information processing facilities must be physically sound—i.e., there must be no gaps in the perimeter or areas where a break-in could easily occur. External walls of the site must be of solid construction, and all external doors must be suitably protected against unauthorised access by control mechanisms, bars, alarms, locks, etc.

c) A staffed reception area or other means of controlling physical access to the site or building must be in place, with access to sites and buildings restricted to authorised personnel only.

d) Physical barriers must, if necessary, be extended from real floor to real ceiling to prevent unauthorised entry and environmental contamination such as that caused by fire and flooding.

e) All fire doors on a security perimeter must be alarmed and must not have hinges that slow closure.

f) Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

g) Visitors to secure areas must be supervised or cleared, with their dates and times of entry and departure recorded. These individuals may be granted access only for specific, authorised purposes, and must be provided with instructions on the area's security requirements and emergency procedures.

h) Access to sensitive information and information processing facilities must be controlled and restricted to authorised personnel only. Authentication controls (e.g., swipe card plus PIN) must be used to authorise and validate all access. An access audit trail must be securely maintained.

i) All personnel must be required to wear a form of visible identification and be encouraged to challenge unescorted strangers and anyone not displaying visible identification.

j) Access rights to secure areas must be regularly reviewed and updated.

k) Critical facilities must be sited to avoid access by the public.

l) Automated mechanisms for environmental control, specifically those dealing with humidity and temperature, must be in place.

m) No obvious signs outside or within the premises must identify the presence of information processing facilities.

n) Support functions and equipment (e.g., photocopiers, fax machines) must be sited appropriately within the secure area to avoid demands for access that could compromise information.

o) Doors and windows must be locked when unattended, and external protection must be considered for windows—particularly those at ground level.

p) Intrusion detection systems must be installed in accordance with professional standards and regularly tested, and must cover all external doors and accessible windows. Alarms at unoccupied areas must be enabled at all times.

q) Directories and internal telephone books identifying locations of sensitive information processing facilities must not be readily accessible by the public.

r) Hazardous or combustible materials must be stored securely at a safe distance from a secure area. Bulk supplies of items such as stationery must not be stored within a secure area until required.

s) Fallback equipment and backup media must be sited at a safe distance to avoid damage if a disaster should occur at the main site.

t) Personnel must only be aware of the existence of, or activities within, a secure area on a need-to-know basis.

u) Unsupervised work in secure areas must be avoided both for safety reasons and to prevent opportunities for malicious activities.

v) Vacant secure areas must be physically locked and checked periodically.

w) Third party support personnel must be granted restricted access to secure areas or sensitive information processing facilities only when required. This access must be authorised and monitored. Additional barriers and perimeters to control physical access may be needed between areas within the security perimeter whose security requirements vary.

x) Photographic, video, audio, or other recording equipment must not be allowed within the secure areas unless formally authorised.

y) Access to a holding area from outside of the building must be restricted to identified and authorised personnel.

z) Holding areas must be designed to allow supplies to be unloaded without delivery staff obtaining access to other parts of the building.

aa) External door(s) of a holding area must be secured when the internal door is opened.

bb) Incoming material must be inspected for potential hazards before it is moved from the holding area to its point of use.

cc) Incoming material must be registered at its time of entry to the site.

5.9.2 SANITISATION POLICY (PE 9.2.4, PE 9.2.6, PE 9.2.7)

a) Storage devices containing sensitive information must be physically destroyed, and non-sensitive information must be securely overwritten rather than removed using the standard delete function.

b) All items of equipment containing storage media such as fixed hard disks must be checked to ensure that sensitive data and licensed software have been removed or overwritten prior to their disposal.

c) Damaged storage devices containing sensitive data may require a risk assessment to determine if they must be destroyed or repaired.

d) Media containing sensitive information must be stored and disposed of securely and safely (e.g., by incineration or shredding) or emptied of data prior to use by another application within the ***[ENTITY]***.

e) Items that could require secure disposal include but are not limited to paper documents; voice or other recordings; CDs, disks, and backup media; output reports; programme listings; test data; and system documentation.

f) It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to isolate the sensitive items. Many organisations offer collection and disposal services for papers, equipment, and media. Care must be taken in selecting a suitable contractor with adequate controls and experience. Disposal of sensitive items must be logged to maintain an audit trail.

5.9.3 EQUIPMENT MOVEMENT POLICY (PE 9.1.7, PE 9.2.5)

a) Information system equipment obtained from third parties must be received in specially designed delivery areas. These areas must not provide direct access to the information system rooms to reduce the possibility of unauthorised access by vendor or delivery personnel.

b) Movement of information system equipment must only be permitted after proper authorisation has been obtained from the responsible System Owner. Guards must verify that authorisation has been granted prior to allowing employees, third party contractors, or visitors to leave the premises with such equipment.

c) Any information system equipment that belongs to a third party or visitor must be registered upon its entry and exit of the premises. Employees may not bring their own information system equipment into the ***[ENTITY]***'s premises unless formal authorisation has been granted.

5.10 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Overview:
The objective of Communications and Operations Management is to establish procedures to manage and operate information processing facilities and assign the responsibilities that govern their management and operation.

5.10.1 OPERATING PROCEDURES POLICY (CM 10.1.1)

a) The Information Systems Division must provide computer operators with documents showing the tasks and responsibilities of employees involved in information systems operations.

b) Operating procedures must be documented and maintained.

c) Management must authorise changes to operating procedures.

d) Documents related to operating procedures must address, at minimum, proper handling of data files (including backups); demands for scheduling of jobs; paper and printout handling; system boot/restart times; application start/stop times; errors, recovery procedures, and corrective actions taken; commands and jobs to be executed; and housekeeping requests for computer consumables.

5.10.2 SEPARATION OF DUTIES POLICY (CM 10.1.3)

a) Information system processes involving sensitive, valuable, or critical information must include controls that outline a separation of duties from start to end—i.e., from initiation to completion. These control measures must ensure that no single individual has exclusive control over information assets and processes. To the fullest extent possible, every task involving sensitive, valuable, or critical information must require at least two people to coordinate information handling activities.

5.10.3 SEGREGATION OF DEVELOPMENT, TEST, AND OPERATIONAL FACILITIES (CM 10.1.4)

a) Development, test, and operational facilities must be segregated to reduce the risks of unauthorised access or changes to the operational system.

5.10.4 THIRD PARTY POLICY (CM 10.2.1, CM 10.2.2)

a) Third party providers of information system services must employ adequate security controls.

b) Appropriate ***[ENTITY]*** officials must approve outsourcing of information system services to third party providers.

c) Service Level Agreements (SLA) must define expectations of performance for each required security control.

d) Security controls compliance of third party providers of information system services must be monitored.

e) Changes to information systems developed by third party providers must be documented and controlled.

5.10.5 CAPACITY MANAGEMENT POLICY (CM 10.3.1)

a) Capacity of all servers must be monitored regularly, and any irregularities reported to the (CISO).

b) Hardware capacity monitoring must include, at minimum, disk space capacity, processor utilisation, main memory, and network interfaces.

c) Trends in usage, particularly in relation to business application or Management Information System (MIS) tools, must be identified. This information must be used to flag and avoid potential bottlenecks that could present a threat to system security or user services, and plan appropriate remedial actions.

d) Needs for additional processing power and storage must be based on the monitoring of actual capacity usage and projections of future capacity demands. These predictions must be validated by System Owners to prevent any system capacity shortages that could affect overall functioning of the services.

e) When acquiring new hardware, rack space, UPS power, and ventilation requirements must be met to ensure that proper capacity is available.

f) The capacity and utilisation of all networks (including dial-up facilities) must be regularly monitored, especially during and immediately after the introduction of new applications and operating systems.

5.10.6 ANTI-VIRUS POLICY (CM 10.4.1A, CM 10.4.1B)

a) Anti-virus software must be installed and enabled on all firewalls, network servers, mail servers, intranet servers, and desktop machines, whether they are in test or production environments.

b) All data imported to a computer via floppy disk, USB, e-mail, file transfer, etc., must be scanned before it is used.

c) Virus signature files must be updated for all machines as released by the anti-virus software vendor.

d) Routine scanning of all files and executables will occur daily on all servers.

e) All files and data received from across a network must be scanned for viruses as they are received.

f) Virus scanning results will be logged, automatically collected, and audited by the system administration/information systems security staff.

g) Employees will inform the System Administrator of any detected virus, configuration change, or unusual behaviour of a computer or application.

h) Any machine thought to be infected by a virus will immediately be disconnected from all networks.

i) Users must be trained to use the anti-virus software.

j) Users must not attempt to remove viruses themselves.

5.10.7 BACKUP POLICY (CM 10.5.1A, CM 10.5.1B)

a) All sensitive, valuable, or critical information residing on information systems must be backed up periodically.

b) Data from applications identified as “sensitive” or “very sensitive” must be backed up at least once per day.

c) Department management must define which information and systems are to be backed up, the frequency of backup, and the backup method on a case-by-case basis.

d) While users are not normally allowed to store information on their workstations, they are responsible for backing up this information if they do.

e) All sensitive, valuable, or critical information recorded on backup computer media (e.g., magnetic tapes, floppy disks, optical disks) and stored outside the ***[ENTITY]*** offices must be encrypted to prevent it from being revealed to or used by unauthorised parties.

f) Backups of sensitive, critical, and valuable information must be stored in an environmentally protected, access-controlled site located at least five miles from where the originals reside.

g) Backups can be recalled from the storage only by authorised personnel using specified authentication methods, and must be delivered to a person other than the one making the request.

h) Disaster recovery sites must be established in a separate location from the primary operations, and have available network and application servers with installed software. A copy of the disaster recovery plan must also be maintained at the disaster recovery site.

i) Critical backups must be verified on separate hardware and audited independently.

j) Sensitive, critical, or valuable information stored on computer media for a prolonged period of time must be tested at least annually to ensure that it is still recoverable.

k) Media for data storage and printouts must be protected from unauthorised use and stored in safe places. A copy must be kept at the disaster recovery site.

l) Procedures for physical access to the disaster recovery site and backup storage site must be of the same level of access as the main computer room.

m) Procedures for removable media must include restoration instructions.

n) Operations department personnel must have a listing of telephone numbers for key vendors, maintenance contractors, telecommunications service providers, department management, and a disaster recovery site. A listing specifying server names and IP addresses of key network devices must be printed and retained by the operations department.

o) Naming conventions for backups as specified in the Removable Media Equipment Procedure must be used.

p) Information must be retained for no longer than is deemed necessary. Backups must be retained in accordance with the following guidelines:

   i. Daily backups must be kept for two weeks.

   ii. Weekly backups must be kept for one month.

   iii. Monthly backups must be kept for one year.

   iv. Yearly backups must be kept in accordance with data retention laws and regulations.

   v. When no longer required, previous content of any reusable media must be erased as specified in the Removable Media Equipment Procedure.

5.10.8 INTERCONNECTION POLICY (CM 10.6.1, CM 10.6.2)

a) Protection of the information system with respect to the integrity and confidentiality of transmitted data across the ***[ENTITY]***'s network must be managed.

b) Information system interconnection agreements must be approved by the appropriate ***[ENTITY]*** officials.

5.10.9 MEDIA MANAGEMENT POLICY (CM 10.7)

a) Information stored on digital media must be sanitised before its disposal or release for reuse to prevent its access and use by unauthorised individuals. Media destruction and disposal must be accomplished in an environmentally approved manner.

b) Media destruction and disposal actions must be tracked, documented, and verified.

c) Information system media—both paper and digital—must be physically controlled and securely stored in accordance with the highest security category of the information it contains.

d) Information system media must be protected until the media are destroyed or sanitised using approved equipment, techniques, and procedures.

e) Information systems must be appropriately labelled as to information in storage, in process, and in transmission.

f) Only authorised users may have access to information in printed form or on digital media removed from the information system.

g) External labels must be affixed to removable information storage media and information system output indicating the information's distribution limitations and handling caveats.

h) System documentation must be protected against unauthorised access.

5.10.10 INFORMATION EXCHANGE POLICY (CM 10.8, CM 10.9.1A, CM 10.9.2)

a) A formally documented system and communications protection policy must be developed, disseminated, and periodically reviewed/updated.

b) Information systems must prevent unauthorised and unintentional information transfer via shared system resources.

c) Information systems must provide non-repudiation capability to determine whether a given individual took a particular action within a specific system.

d) Information systems must reliably associate security parameters (e.g., security labels, markings) with information exchanged between information systems.

e) Information systems media must be controlled while in transit (paper or digital), with the pick-up, receipt, transfer, and delivery of such media restricted to authorised personnel.

f) Known vulnerabilities in the administrative and accounting systems must be reviewed where information is shared between different parts of the ***[ENTITY]***.

g) Sensitive business information and classified documents must be excluded from systems which do not provide an appropriate level of protection.

h) The information system must protect the integrity of transmitted information during electronic transactions.

i) The information system must terminate an online transaction at the end of a session or after a pre-defined time period of inactivity.

5.10.11 MONITORING POLICY (CM 10.10)

a) Information systems must generate audit records for all defined auditable events.

b) The CISO must define auditable events that are adequate to support after-the-fact investigations of security incidents.

c) The information system must provide a capability to compile audit records obtained from components throughout the system into a system-wide (logical or physical), time-correlated audit trail.

d) The information system must capture sufficient information in audit records to establish what events occurred, their sources, and outcomes.

e) Audit logs must be retained for a defined time period to provide support for after-the-fact investigations of security incidents and meet regulatory and ***[ENTITY]*** requirements.

f) Activities of users must be supervised and reviewed with respect to the enforcement and usage of information system access controls.

g) Any unusual information system-related activities and changes to access authorisations must be investigated.

h) Information systems must protect audit information and audit tools from unauthorised access, modification, and deletion.

i) Activities of administrators and operators must be logged with respect to the enforcement and usage of information system access controls.

j) Information system operators must review the daily log file of the systems under their responsibility. A signed printout must be archived for future review if and when such a review becomes necessary.

k) The CISO must periodically verify that audit trails and log files of all system and network applications are being reviewed regularly by the designated personnel.

5.10.12 PATCH MANAGEMENT POLICY (CM 10.10.7, IS 12.4.1)

a) Checks for new security-related patches and updates that are distributed via vendor Web sites must be made at least once every week.

b) Newly released, security-relevant patches, service packs, and hot fixes must be installed promptly after they have been tested for effectiveness and potential side effects on the information systems.

c) The ***[ENTITY]*** must centrally manage its flaw remediation process and install updates automatically without user intervention.

d) The information system must provide time stamps for use in its audit record generation.

e) All released patches and updates that have or have not been installed must be logged. These records would typically include:

   i. Description of the patch/upgrade.

   ii. Date when the patch/upgrade became available.

   iii. Patch/upgrade functionality—which issues does it address?

   iv. Date of installation, or

   v. Reason for not installing.

5.11 IDENTITY AND ACCESS MANAGEMENT

Overview:

The objective of Identity and Access Management is to ensure that good governance is established around the management of user identities within the entity and the respective information to which these users have been granted access.

5.11.1 USER ACCESS MANAGEMENT POLICY (IA 11.1.1, IA 11.2.1, IA 11.2.2, IA 11.2.4)

a) For an employee to obtain information system login credentials, his or her manager must fill out a pre-defined form to request this access. The form must state the name and function of the employee, type and level of access required, a start date, and, where applicable, an end date. These forms must be archived to allow for future review.

b) All employees must sign the Acceptable Use Statement prior to being granted system access. A draft text is found in Chapter 16.

c) Human Resources is responsible for informing the Information Systems Department in a timely manner if an employee is being transferred, promoted, or is leaving the ***[ENTITY]***. In each of these instances, the Information Systems Department must adjust the employee's access rights to reflect the new situation.

d) Allocation of user privileges must be restricted and controlled.

e) User access rights must be reviewed through a formal process at specified intervals to verify application of the ***[ENTITY]***'s access control policies.

5.11.2 PASSWORD POLICY (IA 11.2.3, IA 11.3.1, IA 11.5.1)

a) Users must not share passwords.

b) Passwords must be required for all accounts.

c) The system must provide a mechanism that will notify users to change their passwords.

d) Forgotten passwords must be managed in a secure manner.

e) Passwords provided through a procedure that involves third party knowledge (e.g., some help desk password resetting techniques) must require the password's owner to change it at first use.

f) The system, by default, must not allow the use of null passwords.

g) Passwords must be protected from unauthorised disclosure and modification during storage and transmission.

h) New users must change their passwords the first time they log on to the system.

i) Passwords must not contain any form of the user's name or ID.

j) Passwords for System Administrator (SA) accounts must remain effective for no more than 60 days, and can be set to expire sooner based on assessment of risk and practicality.

k) Passwords for individuals (vs. service accounts) must remain effective for a maximum of 60 days, and can be set to expire sooner based on assessment of risk and practicality.

l) Passwords for contractors must follow the same 60-day requirement or expire at the contract's end minus one day, whichever timeframe is shorter.

m) Service account passwords must expire within 365 days or less.

n) Passwords must not be a word found in a dictionary.

o) Passwords must not be kept in plain view.

p) Passwords must be audited on a regular basis for compliance. This procedure must be strictly controlled, and compromised passwords must be changed promptly.

q) Passwords must contain at least one numeric or special character.

r) Passwords must contain a mixture of at least one uppercase and at least one lowercase letter.

s) Passwords must be at least eight characters long.

t) A password history must be kept to prevent the reuse of, at minimum, the user's previous 24 passwords.

u) The system must not default to displaying a password while logging on.

v) Passwords must not be displayed in clear text as they are being typed.

w) Passwords must not be reusable by the same individual for the same account for a period of at least six months.

x) Minimum password age must be kept to denote different password ages for different types of accounts, to be at least one day.

y) Help Desk employees dealing with lost or forgotten passwords must not provide (reset) passwords without proper identification from the requesting user.

z) The information system must lock out the user once the maximum number of log-on attempts has been reached.

aa) The information system must display an approved system use notification message before granting system access.

bb) Feedback provided by the information system to a user during attempted authentication must not compromise the authentication mechanism.

5.11.3 LOCKOUT POLICY (IA 11.3.2)

a) Inactive terminals in high-risk locations, or which serve high-risk services, must shut down after a defined period of inactivity to prevent access by unauthorised persons.

b) The time-out facility must clear the terminal screen and close both the application and the network session after a pre-defined period of inactivity.

c) The time-out delay must reflect the security risks of the area and the users of the terminal.

d) Restrictions on connection times must be considered to provide additional security for high-risk applications.

5.11.4 CLEAR DESK POLICY (IA 11.3.3)

a) Where appropriate, paper and computer media must be stored in suitable locked cabinets and/or other forms of secured furniture when not in use, especially outside working hours.

b) Sensitive or critical business information must be locked away, preferably in a safe or cabinet, when not required, especially when the office is unattended.

c) Personal computers, computer terminals, and printers must not be left logged on when unattended, and must be protected by key locks, passwords, or other controls when not in use.

d) This policy must take into account the information security classifications, corresponding risks, and cultural aspects of the ***[ENTITY]***.

5.11.5 NETWORK SECURITY POLICY (IA 11.4.1, IA 11.4.2, IA 11.4.3, IA 11.4.5, IA 11.4.6, IA 11.4.7)

a) Users must only be provided with access to the services that they have been specifically authorised to use.

b) Policies on the use of network services must be consistent with the business access control policy.

c) All methods of remote access to the information system must be documented, monitored, and controlled, including remote access for privileged functions.

d) Users are prohibited from attaching modems directly to their computers.

e) Dial-up connections that do not go through designated firewalls are prohibited except when used for authorised testing purposes. Remote maintenance ports (for external vendor support) at the ***[ENTITY]*** must be closed by default, and opened only for the time needed to perform remote maintenance activities.

f) Access to all external networks must pass through an access control point (i.e., firewall) before reaching any intended hosts, and must be subject to authentication.

g) All information must be transmitted in an encrypted format when traversing external (i.e., outside the ***[ENTITY]*** premises) communications facilities. Wireless Local Area Networks (LANs) are allowed only if all transmitted information is encrypted. All wide area access protocols (e.g., telnet, ftp) must be encrypted.

h) Only authorised and approved network devices may be connected to the network.

i) Operational responsibility for networks must be separated from computer operations where appropriate.

j) Systems containing highly sensitive information may be segregated—virtually or physically.

k) Routing controls implemented for networks must ensure that computer connections and information flows do not breach the access control policy of business applications.

l) Use of clear (i.e., unencrypted) passwords to access network devices internally or externally is prohibited.

m) All ***[ENTITY]*** computers that intermittently or continuously connect to an internal or external network must employ encrypted, password-based access controls.

n) All external network connections and network device accesses must be logged and audited on a daily basis.

o) Access to network devices will be authenticated using central access control mechanisms.

p) All network devices and servers must have adequate security patches and service packs applied. Those changes must be tested and approved in accordance with the Change Control Policy.

q) All network changes to ***[ENTITY]*** transmissions and devices must conform to the change Control Policy.

r) All physical network access points must be disabled unless a network device is attached.

s) A session time-out facility that disconnects network terminal devices from associated terminal emulation sessions must be set on all network equipment.

t) Use of network probing and exploring utilities is not allowed unless explicitly authorised.

u) Network monitoring mechanisms must be active to detect, record, and prevent network hacking attempts and denial of service attacks.

v) All network device faults must be logged and monitored on daily basis.

w) All network management passwords must be changed on regular basis.

5.11.6 MOBILE COMPUTING POLICY (IA 11.7.1, IA 11.7.2)

a) Usage restrictions and implementation guidance must be established for wireless technologies, and must document, monitor, and control wireless access to the information system.

b) All mobile computing facilities used for business purposes must be approved by the CISO, who must keep a list of this equipment.

c) Protection (e.g., cryptographic techniques, boot protection) must be in place to avoid unauthorised access to or disclosure of the sensitive information stored and processed by these facilities.

d) Procedures to combat malicious software must be in place and be kept up-to-date.

e) Suitable protection must be given to the use of mobile computing facilities connected to networks.

f) Training must be arranged for staff using mobile computing to raise awareness of the additional risks resulting from this method of working and the controls that must be implemented.

g) Equipment must be available to enable the quick and easy backup of information. These backups must be given adequate protection against theft or loss of business-sensitive information.

h) Mobile computing facilities must also be physically protected against theft—especially when left, for example, in cars and other forms of transportation, hotel rooms, conference centres, and meeting places.

i) When travelling, mobile computing equipment must be carried as hand luggage and disguised whenever possible. Theft must be reported promptly.

5.12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Overview:

The objective of Information Systems Acquisition, Development, and Maintenance is to ensure that information security is applied throughout the complete lifecycle of the information system.

5.12.1 INFORMATION SECURITY ANALYSIS POLICY (IS 12.1.1)

a) Security requirements must be identified and agreed upon prior to the development of an information system.

b) All security requirements, including the need for fallback arrangements, must be identified at the requirements phase of a project, then justified, agreed upon, and documented as part of the service's overall business case.

c) Statements of business requirements for new services, or enhancements to existing services, must specify the requirements for controls.

d) Security requirements and controls must reflect the business value of the information assets involved and the potential business damage that might result from an absence or failure of security.

e) Security requirements and/or security specifications, either explicitly or by reference, must be included in information system acquisition contracts based on an assessment of risk.

5.12.2 DATA VALIDATION POLICY (IS 12.2.1 IS 12.2.2, IS 12.2.3, IS 12.2.4)

a) Data entry to information systems must be restricted to authorised personnel only.

b) Information systems must identify and handle error conditions in an expeditious manner.

c) The structure and content of error messages must be carefully reviewed by the ***[ENTITY]***.

d) Information systems must check information inputs and outputs for accuracy, completeness, and validity.

e) Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) must be in place to ensure that inputs match specified definitions for format and content.

f) Requirements for ensuring authenticity and protecting message integrity in applications must be identified, with appropriate controls also identified and implemented.

g) Output from the information system must be handled and retained in accordance with ***[ENTITY]*** policy and operational requirements.

5.12.3 ENCRYPTION POLICY (IS 12.3)

a) Encryption must be considered for the protection of information processed by information systems categorised as MODERATE or HIGH. The required level of protection must be identified based on a risk assessment that takes into account the type and quality of the encryption algorithm and the length of the cryptographic keys to be used.

b) When implementing the ***[ENTITY]***'s cryptographic policy, consideration must be given to the regulations and national restrictions that might apply to the use of cryptographic techniques.

c) Specialist advice must be sought to identify appropriate level of protection and select suitable products that will provide the protection needed and implement a secure system of key management. In addition, legal advice may need to be sought regarding laws and regulations that might apply to the ***[ENTITY]***'s intended use of encryption.

d) Care must be taken to protect the confidentiality of the private key of a public encryption key pair. This key must be kept secret, since anyone having access can sign documents (e.g., payments, contracts) by effectively forging the signature of the key's owner. Protecting the integrity of the public key is also important, and is provided through use of a public key certificate. Consideration must be given to the type and quality of the signature algorithm and the length of the keys to be used. Cryptographic keys used for digital signatures must be different from those used for encryption.

e) When using digital signatures, consideration must be given to any relevant legislation that outlines conditions under which a digital signature is legally binding (e.g., the legal standing of digital signatures in the realm of electronic commerce). It may be necessary to have binding contracts or other agreements in place to support the use of digital signatures where the legal framework is inadequate. Legal advice must be sought regarding the laws and regulations that might apply to the ***[ENTITY]***'s intended use of digital signatures.

f) Non-repudiation services must be used where it could be necessary to resolve disputes about occurrence or non-occurrence of an event or action (e.g., a dispute involving the use of a digital signature on an electronic contract or payment).

g) To reduce the risks of compromise or loss of cryptographic keys, a management system must be in place to support the ***[ENTITY]***'s use of the two types of cryptographic techniques:

   i. Private key techniques, where two or more parties share the same key, and this key is used to both encrypt and decrypt information. This key must be kept secret since anyone having access to it would be able to decrypt information that was encrypted by this key, or introduce unauthorised information.

   ii. Public key techniques, where each user has a key pair—a public key (which can be revealed to anyone) and a private key (which must be kept secret). Public key techniques can be used for encryption and to produce digital signatures. Both public and private keys must be protected against modification and destruction, and private keys specifically require protection against unauthorised disclosure.

h) Physical protection must be used to protect equipment used to generate, store, and archive keys.

   i. A key management system must be based on an agreed-upon set of standards, procedures, and secure methods for:

   ii. Generating keys for different cryptographic systems and applications.

   iii. Generating and obtaining public key certificates.

   iv. Distributing keys to intended users, including instructions on how keys must be activated when received.

   v. Storing keys, including how authorised users must obtain access.

   vi. Changing or updating keys, to include rules on when keys must be changed and how this will be done.

   vii. Dealing with compromised keys.

   viii. Revoking keys, including how keys must be withdrawn or deactivated (e.g., when keys have been compromised or when a user leaves the ***[ENTITY]***, in which case keys must also be archived).

ix. Recovering keys that are lost or corrupted as part of business continuity management (e.g., for recovery of encrypted information).

x. Archiving keys (e.g., for use with information that has been archived or backed up).

xi. Destroying keys.

xii. Logging and auditing of key management-related activities.

j) To reduce the likelihood of compromise, keys must have defined activation and deactivation dates so they may only be used for a limited period of time. This timeframe must be dependent upon the circumstances under which the cryptographic control is being used, and its perceived risk.

k) Procedures must be considered for handling legal requests for access to cryptographic keys (e.g., when encrypted information may need to be made available in an unencrypted form as evidence in a court case).

l) In addition to the issue of securely managed secret and private keys, the protection of public keys must also be considered.

m) Public key certificates must be used to uniquely bind information related to the owner of the public/private key pair, to the public key.

n) The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g., a certification authority) must cover issues of liability, reliability of services, and response times for service provision.

5.12.4 TESTING POLICY (IS 12.4.1, 12.4.2, IS 12.5.5)

a) Formal testing procedures must be established, and include at minimum the following aspects:

i. Documentation of all authorisation levels, to include a list of authorised information systems personnel to be notified of required modifications, a list of personnel authorised to submit required modifications, authorisation levels for acceptance of the required modifications, and authorisation levels for acceptance of modified applications.

ii. Acceptance by the information system of changes put forward by authorised users only.

iii. Checking of existing security measures and integrity procedures to ensure that they are not being endangered by the modifications.

iv. Specification of all applications, data files, and hardware affected by the modification.

v. User acceptance of all detailed proposals for modification before the information system department begins the development process.

vi. User acceptance of the end result before it is transferred to the production environment.

vii. Updating of system documentation after each modification.

viii. Updating of version numbers for all modified applications.

ix. Logging of all requests for change.

x. Separation of testing into systems integration testing and acceptance testing.

xi. Protection of test data, and rendering it anonymous and randomised when copying it from the production environment.

xii. Testing new programmes that have been modified.

xiii. Providing new version numbers for modified programmes and reports.

b) Where software development is outsourced, the following points must be considered:

   i. Licensing arrangements, code ownership, and intellectual property rights.

   ii. How to certify quality and accuracy of the work carried out.

   iii. Escrow arrangements in the event of third party failure.

   iv. Rights of access to audit the quality and accuracy of completed work.

   v. Contractual requirements outlining the quality and security functionality of code.

   vi. Conducing testing prior to installation to detect malicious code.

5.12.5 SOURCE CODE LIBRARY POLICY (IS 12.4.3)

a) Instructions must be in place that prohibit the placement of libraries of source code in the production environment.

b) A librarian must be assigned for each source code.

c) Access rights of information systems personnel to libraries holding source code must be limited.

d) Instructions must include prohibitions on the storage of source code for applications being modified in the same libraries that hold source code for operating programmes.

e) Written approval of the application owner must be obtained prior to making modifications.

f) All changes made by assigned librarians to libraries that hold source code must be logged.

g) Hard copies of source code must be kept in a secure environment.

h) Old versions of applications must be archived with clear indication of the exact dates and times when they were operational in the form of a printout of the source code directory and reports that must contain at minimum the file name, creation date, date modified, and file size.

i) Periodically (e.g., every two weeks), a new printout of the source code directory must be generated and reconciled with the previous printout.

j) Any differences between printouts must be explained.

k) All printouts must be archived.

5.12.6 CHANGE MANAGEMENT POLICY (IS 12.5.1, IS 12.5.3)

a) All major changes must be defined and prioritised.

b) Modifications to software packages must be discouraged and limited to necessary changes only. All changes must be strictly controlled.

c) The possible consequences of changes must be assessed.

d) Authorisation procedures must be in place regarding how changes should be implemented.

e) Employees and other stakeholders must be informed about the changes.

f) All major changes must be tested prior to their final approval.

g) Procedures and responsibilities must be in place in the event that a change must be reverted.

5.12.7 SYSTEM ACCEPTANCE POLICY (IS 12.5.1)

a) Acceptance criteria for new information systems, upgrades, and versions must be established, with suitable tests of the system carried out prior to acceptance.

b) Acceptance criteria must be defined, documented, and formally reviewed prior to a new system's operational acceptance.

c) All manuals and materials provided to end users while implementation or upgrading software must have management approval.

d) An operations manual that covers start-up, shutdown, and recovery procedures must be made available prior to the introduction of a new system.

e) Specific acceptance is required, and sign-off procedures must be followed, before a programme is developed or modified on a multi-user machine.

f) Every new application or update of an existing application must be introduced to users through a user manual.

g) Every user must complete appropriate training before using a new business application or a new version of an existing business application.

h) New software, as well as new parts of source code (e.g., SQL queries and procedures), must be visually reviewed prior to use whenever possible.

i) Periodic reviews of operating systems must be conducted to ensure that only authorised changes have been made.

j) Operating systems must be updated regularly when a new patch or service pack becomes available—especially in the case of network systems. Responsibility must be assigned for monitoring the Internet, newsgroups, etc., for chatter regarding releases of service packs and security patches.

k) Backup procedures to allow data processing activities to quickly and expediently revert to the previous version of the new system must be developed to enable business activities to continue if a new system fails to meet requirements.

l) Whenever sensitive information will be placed in computers—particularly in computers connected to networks—an analysis of potential security-related impacts must first be performed.

m) Prior to being placed into production use, each new or significantly modified/enhanced business application system must provide a brief security impact statement that has been prepared according to standard procedures.

5.12.8 SOFTWARE INSTALLATION POLICY (IS 12.4.1, IS 12.5.1)

a) Only modifications, no matter how minor, can be installed into a live environment after obtaining the approval of the application owner.

b) Authorisation from department directors must be formally obtained through the use of standard Installation Request Forms.

c) The Installation Request Form must include, at minimum, a reference number linking it to the original request for modification or purchase, and a date by which the application will be required.

d) The applicable librarian must only update libraries holding the operational code after authorisation has been received from the application owner.

e) The production system must only contain executable code. Source code must not be accessible within the production environment.

f) Implementation of production applications must only be made after proper testing, acceptance by the end users, and updates to the libraries that hold the source code.

g) All changes to libraries that hold the operational code must be logged.

h) Previous versions of changed applications must be saved to support a fallback scenario.

5.12.9 VULNERABILITY SCANNING POLICY (RM 3.2.1)

a) Periodic vulnerability scanning must be conducted to achieve ongoing and effective risk management. In cases where the vulnerability scanning is performed by a third party, the arrangement must fall under the conditions outlined by the Third Party Policy.

5.13 INCIDENT MANAGEMENT

Overview:

The objective of Incident Management is the development and subsequent maintenance of a well understood, predictable response to damaging events and computer intrusions.

5.13.1 INCIDENT MANAGEMENT POLICY (IM 13.1, IM 13.2)

a) All significant errors, incomplete processing, and improper processing of production applications must be promptly reported to the ***[ENTITY]***'s Help Desk and the ADG-ISO.

b) A formal reporting and incident response procedure must be established that sets out actions to be taken upon the receipt of an incident report.

c) To ensure a quick, effective, and orderly response to incidents, the individuals responsible for handling information systems security incidents must be clearly defined.

d) The Help Desk must analyse the problems logged and identify their generic root causes or shortcomings to deal with them proactively.

e) If legal action results from an incident, the Help Desk must collect, retain, and present all relevant data to conform to Abu Dhabi's rules for evidence.

f) The Help Desk must record issues as reported by users or operations personnel.

g) An incident must be classified based on its severity and how critical the application systems are. Business owners must be informed immediately in the event of an incident with high severity.

h) The Help Desk must assign appropriate in-house technical support personnel or escalate the problem to a third party if required.

i) If components, such as software or staff, give rise to failures in the information system support structure, the root cause of these failures must be identified to compile a corrective strategy.

j) The CISO must be provided with a summary report of incidents and resolutions on a regular basis.

k) Procedures for addressing information security breaches, business disruptions, or hacker attacks must be prepared and complied with.

l) All employees and contractors must be made aware of the procedure for reporting incidents, and be required to report incidents as quickly as possible to a suitable point of contact, to include:

   i. A list being put in place that contains employees assigned to each application who must be contacted in case of a software/hardware failure

   ii. Instructions to users on recording all symptoms and error messages that appear onscreen

   iii. Instructions to users, if needed, to stop using the computer

   iv. Instructions to disconnect the computer from the network, if necessary (e.g., if viruses are identified)

   v. Instructions to stop using any removable media within the computer in other machines

   vi. Instructions to users on reporting the incident immediately to the Information Security Officer

   vii. Instructions to users to avoid removing or fixing suspicious software or hardware

5.14 BUSINESS CONTINUITY MANAGEMENT

Overview:

The purpose of Business Continuity Management is to create and validate a practiced logistical plan for how the entity will recover and restore partially or completely interrupted critical (urgent) function(s) within a predetermined time after a disaster or extended disruption.

5.14.1 BUSINESS CONTINUITY MANAGEMENT POLICY (BC 14.1.1, BC 14.1.2, BC 14.1.3, BC 14.1.4, BC 14.1.5)

a) A single framework of business continuity plans must be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

b) Each business continuity plan must clearly specify the conditions for its activation and the individuals responsible for executing each of its components.

c) When new requirements are identified, established emergency procedures (e.g. evacuation plans or any existing fallback arrangements) must be amended as appropriate.

d) The business continuity planning framework must consider the following:

   i. Conditions for activation that describe the process to be followed (e.g., situational assessment, who is to be involved) before each plan is activated

   ii. Emergency procedures that describe actions to be taken following an incident which jeopardises business operations and/or human life. These must include arrangements for public relations management and for effective liaison with appropriate public authorities (e.g., police, fire service, local Government).

   iii. Fallback procedures that describe actions to be taken to move essential business activities or support services to alternative temporary locations, and bring business processes back into operation within the required timeframe

   iv. Resumption procedures that describe actions to be taken to resume normal business operations

   v. A maintenance schedule that specifies how and when the plan will be tested, and the process for maintaining the plan

   vi. Awareness and education activities that are designed to create understanding of business continuity processes and ensure that these processes continue to be effective

   vii. Individual responsibilities that outline who is responsible for executing each component of the plan, with alternatives nominated as required

e) Each plan must have a specific owner.

f) Emergency procedures, manual fallback plans, and resumption plans must be within the responsibility of the owners of the appropriate business resources or processes involved.

g) Responsibility for the fallback arrangements for alternative technical services, such as information processing and communications facilities, must generally be assigned to the service providers.

h) Business continuity plans may fail upon being tested, often due to incorrect assumptions, oversights, or changes in equipment or personnel. They must therefore be tested regularly to ensure that they are up-to-date and effective. Such tests must also ensure that all members of the recovery team, as well as other relevant staff, are aware of the plans.

i) The test schedule for business continuity plan(s) must indicate how and when each plan element must be tested. It is recommended to test the individual components of the plan(s) frequently. A variety of techniques must be used to provide assurance that the plan(s) will operate in real life.

j) The test techniques for business continuity plan(s) must include:

   i. Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions).

   ii. Simulations (particularly for training individuals in their post-incident crisis management roles).

   iii. Technical recovery testing (ensuring that the service can be restored effectively).

   iv. Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site).

   v. Testing supplier facilities and services (ensuring that externally provided services and products will meet the contracted commitment).

   vi. Complete rehearsals (testing that the ***[ENTITY]*** personnel, equipment, facilities, and processes are able to cope with interruptions).

k) Techniques used must reflect the nature of the specific recovery plan.

l) Business continuity plans must be maintained by regular reviews and updates to ensure their continuing effectiveness.

m) Procedures must be included within the ***[ENTITY]***'s change management programme to ensure that business continuity matters are appropriately addressed.

n) Responsibility must be assigned for regular reviews of each business continuity plan. Changes in business arrangements not yet reflected in the business continuity plans must be identified and followed by an appropriate plan update. This formal change control process must ensure that updated plans are distributed and reinforced by regular reviews of the complete plan.

6. SAMPLE ROLES AND RESPONSIBILITIES

6.1 ORGANISATIONAL LEAD/CHAIRMAN

The Organisational Lead/Chairman provides strategic leadership, promotes the implementation of information security across the ***[ENTITY]***, and endorses the Information Security Programme.

6.2 CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO is responsible for leading and managing the ***[ENTITY]*** Information Security Programme, with responsibilities that include:

a) Enforcing and monitoring the implementation of, and compliance with, this Information Security Policy.

b) Developing entity-specific programme policies, as necessary.

c) Ensuring that Risk Assessments are conducted for all services.

d) Ensuring that Information Security Plans are developed for all applicable services.

e) Ensuring the implementation of all applicable information security controls as set forth in the Information Security Plan, to ensure adequate security for the respective systems.

f) Ensuring the development of plans for the Security Testing and Evaluation (ST&E) of all applicable services. These plans must be executed by qualified and sufficiently independent organisations (for services categorised as HIGH or MODERATE) to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system's security risk requirements.

g) Serving as the Certifying Official for services that are categorised as HIGH or MODERATE, certifying test results, and providing accreditation recommendations for approval to operate.

h) Supporting ADSIC in developing and implementing an information security awareness campaign, and supplementing the efforts as necessary for the respective entity.

i) Providing information security-related technical training based on the entity's need, and ensuring consistency with the pan-Governmental training programme.

j) Conducting information security communications and outreach by leveraging the Information Security Working Group.

k) Establishing appropriate measures to assess operational capabilities, and determining compliance and effectiveness levels with the Information Security Policy and Information Security Standards.

l) Providing an annual report to the Chairman (or equivalent) and the Information Security Programme Manager of ADSIC on the progress of the entity's Information Security Programme.

m) Coordinating with the leads of other entities, as necessary.

n) Coordinating with ADG-ISO to implement applicable, coordinated incident management procedures, to include the appropriate reporting of incidents to ADG-ISO.

o) Communicating and escalating, as necessary, information security matters to ADG-ISO and ADSIC.

p) Coordinating with other mission assurance programmes to effectively manage risks across the entity, and ensuring continuity of the business.

q) Ensuring that contractors and third party organisations achieve adequate security for the protection of sensitive Government information.

6.3 SYSTEM OWNERS

The System Owner is responsible for defining the application's operating parameters, authorised functions, and security requirements. The Information Owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. In addition, a single system may utilise information from multiple Information Owners.

6.4 DESIGNATED APPROVAL AUTHORITY (DAA)

The Designated Approval Authority (DAA) is the person who formally accredits or accepts the remaining risks to the service. The DAA is a senior Government official of the ADGE, is appointed by the Chairman, and is responsible for the security of all of the entity's services.

6.5 SYSTEM ADMINISTRATOR (SA)

A System Administrator is the person who is in charge of the maintenance and operation of the information system. Some duties of the System Administrator include setting up user accounts, installing software, configuring workstations, etc.

6.6 CONTRACTORS AND THIRD PARTY ORGANISATIONS

Contractors and third party organisations must support the implementation of information security across the ***[ENTITY]***, and in doing so must have the responsibility to protect Government information within their respective purview commensurate with the risk and magnitude of harm that could result from the loss, misuse, unauthorised access to, or modification of such information. Procurement contracts and other agreements between the ***[ENTITY]*** and such contractors and third party organisations must explicitly provide for such protection.

7. OUTLINE BUSINESS CONTINUITY MANAGEMENT PROCEDURES

7.1 OVERVIEW

Business Continuity Management is an interdisciplinary concept used to create and validate a practiced logistical plan for how an organisation will recover and restore partially or completely interrupted critical function(s) within a pre-determined time following a disaster.

7.2 ROLES AND RESPONSIBILITIES

Setting up, maintaining, and executing Business Continuity Management is the responsibility of many different players, including System Owners, senior management, Information System Administrators, information system support staff, end users, and the CISO. Given the large number of people involved, coordination is essential and is best handled by a dedicated Incident Response Team.

7.3 ANALYSIS OF REQUIREMENTS

When developing a Business Continuity Plan (BCP), the first step is to analyse the ***[ENTITY]***'s critical processes, potential threats, and matching impact scenarios. This is usually executed by means of a Business Impact Analysis, in which critical and non-critical ***[ENTITY]*** processes are identified. A process may be considered critical if the expected impact to the ***[ENTITY]*** is considered unacceptable. This estimate will also depend on the cost of establishing and maintaining appropriate business or technical recovery solutions. A process may also be considered critical as a result of regulatory or legal requirements.

Once the Business Impact Analysis is completed, the ***[ENTITY]*** can proceed to formulate its recovery requirements. Here, the ***[ENTITY]*** needs to define its maximum tolerable downtime and recovery time objective in the event of a disaster, as these two variables will drive the building of the technical and organisational solutions in the next phase.

While it is impossible for the ***[ENTITY]*** to foresee all possible disasters, it must still define the most likely impact scenarios and analyse the requirements for each. A practical solution is to begin with the most far-reaching scenario-loss of premises-as other scenarios will be subsets of this.

7.4 DEFINING RESPONSE STRATEGY

This phase consists of identifying the most cost-effective disaster recovery solution that meets the two main requirements from the impact analysis stage:

i. Most critical business functions.

ii. Timeframe in which these functions must be restored.

Business functions do not only refer to information systems, where they would need to be broken down into applications and data, but can also apply to functions outside the applications domain. Examples include the safekeeping of hard-copy information such as legal papers or contracts, and service offerings to the public that do not necessarily require information systems (e.g., certain police services).

In general, the following topics must be addressed when defining the most suitable response strategy:

i. Crisis management command structure.

ii. Location of a secondary work site, (if necessary).

iii. Telecommunications architecture between primary and secondary work sites.

iv. Data replication methodology between primary and secondary work sites.

v. Applications and software required at the secondary work site.

vi. Type of physical requirements at the secondary work site.

7.5 TESTING AND MAINTAINING RESPONSE STRATEGY

After implementing the necessary technical and organisational measures as part of the Business Continuity Plan, the ***[ENTITY]*** needs to test the plan and update it as needed. Testing can range from paper walk-throughs and simulations up to actually testing the various aspects of the plan, for example, restoring business functions on the secondary work site.

The main purpose of testing the Business Continuity Plan is to ensure that it remains valid and to update it if that is not the case. Testing also provides a good way to educate those involved in its execution on their respective roles and responsibilities.

7.6 BUSINESS CONTINUITY PLAN APPENDICES

Appendices included should be based on systems and plans requirements.

a) Personnel Contact List.

b) Vendor Contact List.

c) Equipment and Specifications.

d) Service Level Agreements and Memorandums of Understanding.

e) Information System Standard Operating Procedures.

f) Business Impact Analysis.

g) Related Contingency Plans.

h) Emergency Management Plan.

i) Occupant Evacuation Plan.

j) Continuity of Operations Plan.

8. OUTLINE CHANGE MANAGEMENT PROCEDURES

8.1 OVERVIEW

The goal of Change Management is to ensure that changes to services and/or systems are handled in a controlled manner, according to standardised methods and procedures, with the purpose of reducing their impact to the services. Most changes introduce additional risks which, if uncontrolled, could negatively effect the service level of the ***[ENTITY]***. Change Management is a tool for managing these risks.

Changes can affect desktop computers, the network and network devices, servers, databases, and other information system assets. Small changes typically do not require a formal change management process, as their associated risks do not generally warrant the expenses that result from change management process adoption. A risk-based decision needs to be made as to whether or not a proposed change should trigger a formal Change Management Process.

8.2 ROLES AND RESPONSIBILITIES

The Change Management process is usually overseen by a Change Review Board made up of representatives from key organisational areas. These can include information system staff, the Chief Information Security Officer (CISO), and other selected employees based upon the specific type of change.

8.3 PRIORITISING CHANGES

A formal procedure for submitting and recording change requests should be established to help the Change Review Board prioritise the requests that they receive. Only changes from authorised submitters should be considered. A recommended practice is to allow changes to be submitted by any employee provided a representative from a pre-determined level of management co-signs the request.

Accepting and prioritising received changes requires a big-picture view of the ***[ENTITY]***, its mission, best practices, and available resources. Only requests for change that do not conflict with these areas should be accepted and prioritised.

8.4 PLANNING CHANGES

The change planning process normally consists of estimating the needed resources financially as well as in terms of employee hours and specialties. This estimation should involve careful evaluation of the scope, impact, and complexity of the proposed change.

An important part of the planning phase is defining a fallback scenario to use in the event that a planned change must be reverted.

8.5 TESTING CHANGES

Like any change to the ***[ENTITY]***'s services, the proposed change must be assessed in a test environment that closely mimics the production environment. Testing should encompass both the change itself and the fallback scenario.

8.6 COMMUNICATING CHANGES

Since the Change Management process applies only to major changes that significantly impact the ***[ENTITY]***, clear and timely communication is key to assuring change acceptance. The Help Desk can be mobilised to provide support following the change's implementation. Communicating a proposed change could produce responses from other organisational units on potentially negative impacts to their services which may not have been realised earlier in the Change Management process.

8.7 IMPLEMENTING AND DOCUMENTING CHANGES

Change implementation should follow pre-defined procedures and proceed according to a formal implementation plan that includes criteria to trigger the fallback scenario if the change fails to meet its objectives.

Documentation of the full Change Management process is essential, and typically includes the following elements:

i. Initial request for change.
ii. Change approval.
iii. The priority of the change.
iv. Test plan, implementation plan, and fallback scenario.
v. Date/time of implementation.
vi. Persons responsible for implementation.
vii. Whether implementation succeeded, failed, or was postponed.

8.8 POST-IMPLEMENTATION REVIEW OF CHANGES

Once the Change Management process has been completed, the Change Review Board will evaluate the change, identify shortcomings in the process, and propose remediation actions to be taken prior to the next change. A post-implementation review should be conducted after both successful and unsuccessful changes. For the latter, the review process should be expanded to facilitate full understanding of why the change process did not produce the desired outcome.

9. OUTLINE PATCH AND VULNERABILITY MANAGEMENT PROCEDURES

9.1 OVERVIEW

Patch and Vulnerability Management is undertaken to ensure that computer systems attached to the ***[ENTITY]***'s network are updated accurately and in a timely manner with security protection mechanisms (patches) for known vulnerabilities and exploits. These patches are intended to reduce or eliminate vulnerabilities and exploits and have a limited impact on the ***[ENTITY]***.

Many attempted exploits are successful because organisations have not patched and updated their systems in a complete and timely manner. A comprehensive set of Patch and Vulnerability Management procedures will help lower the risks associated with known flaws by reducing the time between a flaw's identification and remediation.

Key areas that are part of the Patch and Vulnerability Management process include:

i. Keeping an accurate inventory of all information system assets.
ii. Monitoring for vulnerabilities, flaws, and threats.
iii. Identifying and prioritising relevant vulnerabilities, flaws, and threats.
iv. Testing patches and updates.
v. Deploying patches and updates.

9.2 ROLES AND RESPONSIBILITIES

Most of the work involved in the Patch and Vulnerability Management process will be carried out by System and Network Administrators in close collaboration with the CISO. It is recommended that a Patch Manager be appointed to be responsible for the overall process.

9.3 INVENTORY KEEPING

Having an up-to-date inventory of all information system assets is essential to a successful Patch and Vulnerability Management programme. The Patch Manager should use the existing inventory of ***[ENTITY]*** assets and manually supplement any information system asset that is not captured in the ***[ENTITY]***'s inventory system.

Prior to the Accreditation phase of the overall Risk Management process, this inventory database should be updated with all information system asset information relevant to the service being accredited. This will ensure that the asset database is always up to date and reflects assets belonging to all officially allowed systems. Documentation is recommended to include, at minimum, the following properties of each information system asset:

a) Associated system name.
b) Property number.
c) Owner of the information system resource (i.e., primary user).
d) System Administrator.
e) Physical location.
f) Connected network port.
g) Hardware details (e.g., central processing unit, memory, disk space, Ethernet addresses (i.e., network cards), wireless capability, etc.)

h) Software details (e.g., operating system and version number, software packages and version numbers, network services, Internet Protocol (IP) address (if static), input/output ports, firmware version, etc.)

Since keeping track of all of these assets is a daunting task when done manually, it is recommended that automated tools feeding into a central database be installed to monitor quantities of workstations, network devices, and servers. These tools can typically assist in deploying patches across workstations and other devices as well.

The inventory system must allow for grouping of assets by owner or ***[ENTITY]*** units, and via interconnection with other assets to quickly determine which employees, departments, or systems would be affected by a specific vulnerability.

9.4 MONITORING FOR VULNERABILITIES

The Patch Manager is responsible for keeping abreast of the latest vulnerabilities for each system under the ***[ENTITY]***'s control. Useful sources of information can include vendor alerts, newsletters, e-mails, Web sites, etc. Another, more specific approach for identifying vulnerabilities is to periodically execute a vulnerability scan on the information system's assets.

9.5 IDENTIFYING AND PRIORITISING RELEVANT VULNERABILITIES

Given the large number of potential vulnerabilities, the Patch Manager is confronted with numerous new patches every day. However, not all of these patches are relevant, and irrelevant patches could actually compromise the system they are intended to remediate. Carefully selecting relevant vulnerabilities that need patching is a difficult yet important activity.

Identification and prioritisation of these relevant vulnerabilities should be based on the following three criteria:

i. Implication of the vulnerability: which systems are exposed, and what would be the impact should the vulnerability be successfully exploited?

ii. Presence of exploits: a vulnerability is only a problem if it can be exploited. The more exploits have occurred, the more urgent patching becomes.

iii. Risk assessment of patching vs. non-patching: deciding to deploy the available patch should be the result of weighing the benefits of being protected against the risk of disrupting the system and/or the damage from the vulnerability being exploited.

9.6 TESTING PATCHES AND UPDATES

Patches and updates may only be installed in the production environment after successful testing to ensure they do not negatively affect the system (or other, interconnected systems) they are intended to enhance. It is good practice to take the following steps:

i. Validate download: often vendors offer patches as downloads on their Web sites. The Patch Manager must validate the authenticity of the download source as well as the download itself (e.g., by using checksums if available).

ii. Scan the download for viruses or malware: as a precaution, always allow anti-virus software to evaluate any download onto the ***[ENTITY]***'s system, including patches and updates.

iii. Test patches in a separate environment: to prevent a patch or update with unintended negative impact on the ***[ENTITY]***'s system from causing damage, it is best practice to test patches and updates on a test server that is not connected in any way to the production environment.

iv. Inter-dependency of patches: certain patches require the installation of other patches as prerequisites to function properly. If these patches are not presently installed, it could affect the usefulness of the selected patch.

v. Learn from others: a practical approach to learn about the potential dangers and unwanted implications of patches is to search the Internet and other sources, such as user groups, for the experiences of others with a particular patch.

vi. Decide to install or not: if a major concern surfaced during any of the above steps, it might be wise not to install the patch. However, this will require a careful evaluation of the expected benefits of installing the patch vs. accepting the presence of the unaddressed vulnerability within the system.

9.7 DEPLOYING PATCHES AND UPDATES

Once the decision has been made to remediate selected vulnerabilities, the Patch Manager has three options:

i. Install the security patch: while this is the most straightforward way to address the vulnerability, this option depends on the availability of a security patch that is usually provided by the vendor of the application.

ii. Modify the configuration of a security control: this option is practical in certain situations where, e.g., the modification of a firewall rule will eliminate the threat.

iii. Remove the vulnerable software: if the software that is vulnerable to threats is not needed, the best way to address the vulnerability is to remove the software. This option is usually applicable when installing new systems whose defaults include additional programmes and services that are not always needed.

The final step in the deployment phase is to validate that all changes made to the information system have been successful. This can be accomplished by such measures as reviewing log files, using a vulnerability scanning tool to actively evaluate the patched system, and writing specific exploit code to test the effectiveness of the patch or update.

10. OUTLINE INFORMATION SYSTEMS ACQUISITION MANAGEMENT PROCEDURES

10.1 OVERVIEW

This document provides procedures for the Acquisition Management of products and services to ensure that all acquisitions comply with the ***[ENTITY]***'s Information Security Policy and ensure a consistent approach to acquiring information security products and services. Without a comprehensive Acquisition Management procedure, acquired information system products and services could inadvertently introduce new vulnerabilities and threats to the ***[ENTITY]***.

10.2 ROLES AND RESPONSIBILITIES

The Application Owner of each system is responsible for purchase decisions related to that system, and the role of the CISO is to verify that all purchases are made in accordance with the standards contained within this document. This ensures that newly purchased information system equipment and services do not negatively impact existing information system assets.

The actual purchasing, requesting/evaluating Requests for Proposal, selection of vendors, and related functions may be handled by a dedicated Purchasing Office, if one is available.

10.3 SUBMIT REQUEST FOR PURCHASE

All new purchases involving information system products and services above an ***[ENTITY]***-defined amount should be entered on a Request for Purchase form, which is then submitted to the Application Owner. Only approved employees may submit a Request for Purchase, and these forms must be registered to ensure they are duly processed.

10.4 APPROVE REQUEST FOR PURCHASE

The Application Owner must approve the request for purchase. From an information security point of view, most important is that the requested product or service is in line with the existing infrastructure and will not introduce additional risks to the ***[ENTITY]***. The Application Owner should also verify that the information system department is able to offer sufficient support, particularly if the product or service is new to the ***[ENTITY]***.

10.5 OBTAIN QUOTES

After the Application Owner has approved the Request for Purchase, the Purchasing Officer will send out Requests for Quotation to selected vendors. These vendors have been chosen based on the products/services being requested as well as such factors as the vendor's reputation, financial position, ability to offer local support, and past experience.

10.6 SELECT VENDOR

In general, vendor selection should be based on a price versus quality evaluation. Depending on the size and criticality of the required goods or services, additional considerations-such as previously supplied products or an intention to develop a long-term relationship—might also play a role.

10.7 RECEIVE PRODUCT OR SERVICE

Among the most important steps within the acquisition process is the actual receipt of the purchased products or services. The ***[ENTITY]*** should follow a formal change management procedure in the

event of a major purchase. In all situations, the newly acquired product must be tested prior to being transferred to the production environment.

10.8 UPDATE VENDOR DATABASE

After taking delivery of the requested product or service, the ***[ENTITY]*** must update its vendor database to reflect both positive and negative aspects of the acquisition. This information will be used as input on a subsequent purchase cycle.

10.9 THIRD PARTY ACQUISITION

The steps above can also be applied to the purchase of third party products and services, with one significant difference: in third party acquisitions, a service level agreement should be in place to allow the ***[ENTITY]*** to continuously monitor the quality of services received. This agreement should address, at minimum, the following elements:

i. Definition of services.
ii. Performance measurement.
iii. Problem management.
iv. Escalation process.
v. Entity duties.
vi. Warranties.
vii. Disaster recovery.
viii. Termination of agreement.

11. OUTLINE INCIDENT MANAGEMENT PROCEDURES

11.1 OVERVIEW

The purpose of Incident Management response procedures is to ensure a consistent approach to handling information security incidents to minimise loss, and restore services. Without these comprehensive response procedures in place, a malfunctioning information system may not be restored in a timely manner, and critical data might be lost. These procedures should incorporate lessons learned from past incidents to help prepare for future incidents.

11.2 ROLES AND RESPONSIBILITIES

In most cases, the primary responsibility for responding to incidents will be with the System Administrator, who must closely collaborate with the owner of the affected system and the CISO.

If an incident affects multiple entities, cross-entity coordination with counterparts could be required.

11.3 SETTING UP INCIDENT MANAGEMENT

To enable the ***[ENTITY]*** to effectively deal with incidents, it is essential to establish an organisational infrastructure, supported by tools, to aid those individuals responsible for Incident Management. Typical elements that can be assembled in advance include contact lists; escalation procedures, calling trees, emergency telephones, flashlights, a fully equipped war room for coordinating a response; and laptops pre-loaded with boot images, recovery software, and other relevant tools.

Although not technically part of Incident Management, prevention is usually the best defence. Decreasing the chance of incidents is a more effective way of lowering risks for the ***[ENTITY]***. Prevention activities should be focused on the following areas:

i. Patch management: a fully patched system offers additional protection against malicious users.

ii. Host and network security: besides patching the information system, hardening the host and network through secure configuration management helps prevent incidents, and should be performed for all systems under the ***[ENTITY]***'s control.

iii. Malicious code prevention: use of anti-virus and anti-malware filtering software reduces the opportunities for malicious code to do damage, and lowers the number of incidents.

iv. User awareness and training: users should be made aware of the role they can personally play in preventing incidents.

11.4 DETECTING INCIDENTS

Given that the number and variety of potential incidents is overwhelming, the ***[ENTITY]*** is best served by preparing for a set number of incident categories and developing standard response procedures for each. A recommended breakdown includes:

CATEGORY	TYPE	DESCRIPTION
Category I	Unauthorised Access	Involves intentional or unintentional unauthorised access to data, whether in electronic or physical form. This also includes loss or theft of a device known to store, process, or transmit data classified as for official use or confidential information.
Category II	Denial of Service	Activity that impairs, impedes, or halts the normal functionality of a system or network. Can be technical (e.g., network-based attack) or physical (e.g., a fire).
Category III	Improper Usage	Encompasses activities that due to actions (of either configuration or usage) make systems potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliant or improper configuration changes or handling by authorised users.
Category IV	Malicious Code	Installation of malicious software (e.g., Trojan, backdoor, virus, botware, spyware, worm).
Category V	Combination of the above	Incidents are not always easy to classify, since many consist of a combination of the categories described above.

Table 3: Categories of Incidents

Detecting incidents can often be challenging, especially when they involve malicious activities that have been done on purpose with the intention of not alerting the ***[ENTITY]***. The sheer volume of potential incidents requires an extensive effort to weed out the false positives, and often specialised tools and expertise are needed to detect advanced attacks. This can make detection a difficult task.

To facilitate the detection process, the ***[ENTITY]*** can take certain steps to reduce the efforts required and increase the detection timeframe. Setting up a baseline of normal system behaviour is beneficial, as it allows the ***[ENTITY]*** to detect any deviation from the baseline—which can be considered to be an indication of potential incidents. Using centralised analysing facilities to correlate logs from different sources is another way of improving the chances of detecting anomalies that could be warning signs of an incident.

Once the ***[ENTITY]*** has established that an incident is in progress or has occurred, it is important to begin documenting the situation and collecting evidence to assist in troubleshooting and provide support if disciplinary actions or lawsuits are required at a later date. The entity should also prioritise the incident to allocate a proper amount of time and resources to address the situation. Prioritisation should take into consideration the immediate and future effects of the incident, as well as the criticality of information system assets that are or will be impacted.

As a final step in the discovery phase, the ***[ENTITY]*** should notify all relevant stakeholders who are or will be affected by the incident.

11.5 RESPONDING TO INCIDENTS

Key to effective incident response is to contain any future damage, followed by repairing the damage that has already been done. Selecting an appropriate containment response depends on the category of the incident. As explained earlier, the ***[ENTITY]*** should have a response strategy in place for all major categories to bring down response time and prevent unnecessary additional damage.

Throughout its response, the ***[ENTITY]*** should document its steps and collect and archive all relevant evidence to assist with future incidents and use in possible legal steps the ***[ENTITY]*** might eventually take.

Damage repair usually involves restoring backups, images, and configurations of the affected information system assets. A robust backup process will greatly help during this phase.

The following two tables clarify the escalation procedure to be followed in the event of an incident. The escalation path and recommended time frames are included for each category listed in Table 1 of paragraph 11.4.

TIER	PERSONS TO BE NOTIFIED
1	Help Desk
2	System/Security Administrator
3	System Owner
4	Entity CISO
5	ADSIC CISO

Table 4: Reporting Hierarchy

CATEGORY	SEVERITY	INITIAL PHONE REPORT	INITIAL WRITTEN REPORT	MINIMUM REPORTING
(I) Unauthorised Access	Severe	15 minutes	4 hours	Tier 5
(I) Unauthorised Access	Moderate	2 hours	8 hours	Tier 4
(I) Unauthorised Access	Low	4 hours	16 hours	Tier 3
(II) Denial of Service	Severe	15 minutes	4 hours	Tier 5
(II) Denial of Service	Moderate	2 hours	8 hours	Tier 4

CATEGORY	SEVERITY	INITIAL PHONE REPORT	INITIAL WRITTEN REPORT	MINIMUM REPORTING
(II) Denial of Service	Low	4 hours	16 hours	Tier 3
Improper Usage (III)	Severe	4 hours	12 hours	Tier 4
(III) Improper Usage	Moderate	8 hours	24 hours	Tier 3
(III) Improper Usage	Low	16 hours	48 hours	Tier 2
(IV) Malicious Code	Severe	15 minutes	4 hours	Tier 5
(IV) Malicious Code	Moderate	2 hours	8 hours	Tier 4
(IV) Malicious Code	Low	4 hours	12 hours	Tier 3
(V) Combination of the Above	N/A	2 hours	As soon as possible	Tier 4

Table 5: Incident Reporting Times

In most cases, the first two tiers will need to be included as the first reports are being filed. Further escalation is typically initiated by Tier 1 and Tier 2, depending on the incident's severity. For each incident, a careful evaluation of the escalation path must to be made, that depends on the categorisation of the service affected by the incident.

The following steps should be provided as the incident is being escalated:

a) Incident category.

b) Current status of the incident.

c) Summary of the incident.

d) Affected system and data.

e) Actions taken on the incident by all incident handlers.

f) Contact information for other involved parties (e.g., System Owners, System Administrators).

g) List of evidence gathered during the incident investigation.

h) Comments from incident handlers.

i) Next steps to be taken (e.g., waiting for a System Administrator to patch an application).

11.6 POST-INCIDENT EVALUATION

Once the situation has been sufficiently contained and the damage has been repaired, the ***[ENTITY]*** should take time to evaluate the incident and how the response was executed. This activity will form the basis for lessons learned, and when done properly, can lead to a better response for subsequent situations.

12. OUTLINE HUMAN RESOURCES SECURITY PROCEDURES

12.1 OVERVIEW

The objective of Human Resources Security procedures is to ensure that employees, contractors, and third party users understand their responsibilities and are suitable for the roles for which they are being considered, thus reducing the risks of theft, fraud, and facilities misuse.

12.2 ROLES AND RESPONSIBILITIES

Most employee screening activities are carried out by the Human Resources Department, while all employees bear the responsibility of acting in accordance with the ***[ENTITY]***'s information security policy.

12.3 BACKGROUND CHECKS

Appropriate background verification checks—also known as "screening" or "clearance"—should be carried out for all candidates for employment, contractor status, or third party user status. This process includes checks that:

i. Are commensurate with the ***[ENTITY]***'s needs, and with relevant legal and regulatory requirements.

ii. Take into account the classification/sensitivity levels of the information to be accessed, and its perceived risks.

iii. Take into account all privacy, protection of personal data, and other relevant employment legislation.

iv. Include, where appropriate, components such as identity verification, character references, CV verification, and criminal/credit checks.

12.4 TERMS AND CONDITIONS OF EMPLOYMENT

Employees, contractors, and third party users must agree to and sign a statement of rights and responsibilities for their affiliation with the ***[ENTITY]***, including rights and responsibilities with respect to information security. Controls included in the signed agreement include, at minimum:

i. Information on the scope of access and other privileges to be granted to the applicant, with respect to the ***[ENTITY]***'s information and information processing facilities.

ii. Information regarding the applicant's responsibilities under legal and regulatory requirements and organisational policies as specified in this or other signed agreements.

iii. As appropriate, information on responsibilities for the categorisation of information and management of organisational information facilities that the applicant may use.

iv. As appropriate, information on the handling of sensitive information, both internal to the ***[ENTITY]*** and that which is received from or transferred to outside parties.

v. Information regarding responsibilities that extend outside the ***[ENTITY]***'s boundaries (e.g., for mobile devices and teleworking).

vi. Information on the ***[ENTITY]***'s responsibilities for handling of information related to the applicant that is generated in the course of an employment, contractor, or other third party relationship.

vii. Actions that can be anticipated, under the ***[ENTITY]***'s disciplinary process, as a consequence of failure to observe security requirements.

These controls may include the provision of an ***[ENTITY]*** code of conduct or code of ethics to the employee, contractor or third party. They may also include a requirement to sign, prior to being provided access or other privileges to information or information processing facilities, a separate:

i. Confidentiality or non-disclosure agreement

ii. Acceptable Use Policy

12.5 DURING EMPLOYMENT

It is imperative to ensure that employees, contractors, and third party users are aware of both information security threats and concerns and their personal responsibilities and liabilities. These individuals must be properly equipped to support ***[ENTITY]***'s security policy in the course of their normal work and reduce the risk of human error. These responsibilities can be divided into three areas:

A. Management Responsibilities

Management should require employees, contractors, and third party users to apply security controls in accordance with established policies and procedures of the ***[ENTITY]***. Suggested controls include:

i. Appropriately informing all employees, contractors, and third party users of their information security roles and responsibilities prior to granting access to sensitive information or information systems (see 12.4, Terms and Conditions of Employment).

ii. Providing all employees, contractors, and third parties with guidelines/rules that state the security control expectations of their roles within the ***[ENTITY].***

iii. Achieving an appropriate level of awareness of security controls among all employees, contractors, and third parties that is relevant to their roles and responsibilities, and the appropriate level of skills and qualifications to execute those security controls.

iv. Assuring conformity to the terms and conditions of employment that are related to security.

v. Motivating adherence to the security policies of the ***[ENTITY]***, e.g., as with an appropriate sanctions policy.

vi. Mitigating the risks of a failure to adhere to policies by ensuring that all persons have appropriately limited access to the ***[ENTITY]***'s information and information facilities.

B. Information Security Awareness, Education, and Training

All employees of the ***[ENTITY]***, and where relevant contractors and third party users, should receive appropriate awareness training in, and regular updates of, ***[ENTITY]*** policies and procedures relevant to their job functions. Suggested controls include:

i. A formal induction process that includes information security training prior to being granted access to information or information systems.

ii. Ongoing training in security control requirements; legal and regulatory responsibilities; and the procedures suitable to personal roles and responsibilities.

iii. Periodic reminders that cover both general security topics and specific issues of relevance to the ***[ENTITY]***.

iv. Other appropriate efforts to raise and maintain awareness of security issues.

C. Disciplinary Process

A formal disciplinary process should be in place for employees who have committed a security breach. Suggested controls include:

i. A reasonable evidentiary standard to initiate investigations (reasonable suspicion that a breach has occurred).

ii. Appropriate investigatory processes, including specification of roles and responsibilities, standards for collection of evidence, and chain of custody of evidence.

iii. Disciplinary proceedings that observe reasonable requirements for due process and quality of evidence.

iv. A reasonable evidentiary standard to determine fault that ensures correct and fair treatment for an individual suspected in a breach.

v. Sanctions that appropriately take into consideration factors such as the nature and gravity of the breach, its impact on operations, whether it is a first or repeat offence, whether or not the violator was appropriately trained, and whether or not the violator exercised due care or exhibited negligence.

vi. An overall process that functions as both deterrent and sanction purposes.

12.6 TERMINATION OR CHANGE OF POSITION

The purpose of establishing termination procedures is to ensure that employees, contractors, and third party users exit the ***[ENTITY]***, or transition to new employment responsibilities within the ***[ENTITY]***, in an orderly manner.

Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. Suggested controls include:

i. Changes of responsibilities and duties within the ***[ENTITY]*** are processed as a termination (of the old position) and re-hire (to the new position), using standard controls for those processes unless otherwise indicated.

ii. Other employees, contractors, and third parties are appropriately informed of a person's changed status.

iii. Any post-employment responsibilities are specified in the terms and conditions of employment, or as part of the contractor or third party contract.

All employees, contractors, and third parties should return all ***[ENTITY]*** assets in their possession upon termination of the employment relationship or contract. Suggested controls include:

i. Formalisation of the process for return (e.g., checklists against inventory).

ii. Inclusion in this requirement of ***[ENTITY]*** hardware, software, and data of any kind.

iii. When the employee, contractor, or third party uses personal equipment, secure erasure of software and data belonging to the ***[ENTITY]***.

Access rights to information and information systems should be removed upon termination of the employment or contractual relationship. Suggested controls include:

i. Changes of employment or contractual status include removal of all rights associated with prior roles and duties, and creation of rights appropriate to the new roles and duties.

ii. Removal or reduction of access rights prior to the termination where risks indicate this step to be appropriate (e.g., where termination is initiated by the ***[ENTITY]*** or access rights involve highly sensitive information or facilities).

13. OUTLINE EVENT MANAGEMENT PROCEDURES

13.1 OVERVIEW

Event Management is the overall term for collecting and analysing security events on an information system. With Event Management procedures in place, the ***[ENTITY]*** is able to identify and counteract security risks in a timely manner.

Event Management uses automated tools to collect data about events on the system, usually from a wide range of log files—system logs, application logs, firewall logs, intrusion detection logs, and more. Because of these disparate sources, correlation functionality is used to link events that extend across the different log files.

The purpose of collecting log file information is to analyse historical trends and identify any deviations from those trends that might indicate a security breach. In addition, a comprehensive log, or audit trail, of the system allows the ***[ENTITY]*** to monitor user activities—which enhances the individual accountability of each user.

Since log files are often very large, automated tools are needed to assist the ***[ENTITY]*** in capturing and normalising them, and extracting relevant information. Specialised software, usually known as Security Event Manager (SEM) or Security Information and Event Manager (SIEM), is used to help the ***[ENTITY]*** manage its log files.

13.2 ROLES AND RESPONSIBILITIES

System Administrators, Network Administrators, Firewall Administrators, and others in similar positions are responsible for setting up and maintaining security logs on their respective systems. The Chief Information Security Officer (CISO) is responsible for overseeing these administrators and for analysing their log files.

13.3 LOG FILE CONFIGURATION

Configuring these log files is one of the most important steps within the Event Management process. Failing to capture enough information, or failing to record all relevant events, can severely impact the analysis of the files. Conversely, capturing too many events can make the analysis phase unduly difficult and negatively affect server performance.

The System Administrator should set up the log file configuration in close collaboration with the CISO to determine the best approach. This can vary based on available configuration settings, system sensitivity, applicable policies, and any laws that may require event logs to capture specific levels of detail.

The log file configuration process can be broken down into three phases:

i. Log generation: defines the amount of data to be captured by carefully balancing system performance and organisational need for detail.

ii. Log storage: regulates how and where to store the log files-on the system itself, on a dedicated log file server, or not at all (e.g., in the case of a low-risk system). Use of a standard format is preferred, as this facilitates the correlation of log files between different systems.

iii. Log security: covers log file access rights, secure handling (e.g., when transferring log files to a different server), and actions to be taken if logging cannot take place (e.g., stopping the application).

13.4 LOG FILE ANALYSIS

After the relevant data has been captured, the next and most important step is to analyse the resulting log files. While this can be challenging at first, having a robust tool to record, store, and process these files will aid in filtering out data that could indicate a security threat. Analysis of log files involves the following steps:

i. Understanding the log files: since log files can sometimes be cryptic or difficult to read, it is important to gain a solid understanding of their content and context. This will help weed out false positives and allow the ***[ENTITY]*** to focus on truly important events.

ii. Prioritising log events: once full understanding of the log files has been obtained, the next step is to prioritise the events according to their importance, generating system, certain critical users, and other relevant criteria.

Another important consideration in the log file analysis phase is the location and role of the system being logged. Event logging that takes place at the information system infrastructure level of the ***[ENTITY]*** requires a different approach than does logging of an isolated application. Application Event Management is usually tailored to a specific application, whereas Event Management at the infrastructure level is typically more standardised. Also, the latter would focus more on compliance with ***[ENTITY]*** policies while the former would focus on correct use of the application.

13.5 INCIDENT RESPONSE

The ***[ENTITY]*** must relate its Event Management processes to its incident response procedures to properly elevate suspicious events. When starting with Event Management, many false positives will be generated because the event analysis phase is not yet fully attuned to the specifics of the ***[ENTITY]***. It is therefore recommended to take a careful approach and only refer events to the incident response team that have been ruled out as being false positives.

13.6 OTHER CONSIDERATIONS

The ***[ENTITY]*** must set up timeframes for keeping event records to enable administrators to organise their backups and storage activities accordingly. The ***[ENTITY]*** must also determine the format in which the logs should be kept to ensure future usability, and whether or not the files should be encrypted.

In addition, the ***[ENTITY]*** should periodically verify that log configurations of all relevant systems are still up-to-date, and that logging continues to take place as intended.

14. OUTLINE BACKUP PROCEDURES

14.1 OVERVIEW

The purpose of Backup Procedures is to ensure a consistent approach to backing up all data needed to restore a system in the event of an incident. Without comprehensive backup and restore procedures, the information system may not be restored in a timely manner and/or important data may be forever lost. Generally speaking, backing up data serves two purposes: first, to restore a system to its previous state following a disaster; and second, to restore small numbers of files that have been accidentally deleted or corrupted.

14.2 ROLES AND RESPONSIBILITIES

Systems Administrators are usually responsible for performing backups according to the procedures contained within this document. The Chief Information Security Officer (CISO) is responsible for monitoring backup procedure compliance.

14.3 BACKUP CONTENT

The first step of setting up a backup strategy is to determine which systems and which data belonging to these systems should be included in the backup. This can include operating system files, database files, database contents, configuration settings, user information such as preferences, and more.

Selection depends upon the criticality of the system, the frequency of change (static vs. dynamic systems), and financial/operational considerations. Not all data has equal importance, and the backup strategy should reflect the data classification schema currently in place for the ***[ENTITY]***.

Another consideration is the type of backup—full vs. incremental. A full backup consists of making a backup of all data, while an incremental backup only backs up changes that have been made since the last backup. Incremental backups are usually much smaller in size, and are consequently faster to execute, but the restoration process is more cumbersome and prone to errors since multiple backups must be combined to restore the original data.

14.4 BACKUP FREQUENCY AND RETENTION

The frequency chosen for backups depends upon the number of transactions taking place on the system as well as the system's criticality. Most backups take place on a daily basis, but for highly critical systems a more frequent schedule can be followed.

Special consideration should be given to applicable retention laws to determine types of data that can be stored, and for how long.

The following is an example of a common backup scheme:

Daily backups	One tape for every weekday (e.g., Sunday tape, Monday tape, etc.)
Weekly backups	Five tapes, one for each week
Monthly backups	Twelve tapes, one for each month
Yearly backups	To be stored in accordance with applicable retention laws

Table 6: Example of a Backup Scheme

14.5 BACKUP LOGISTICS

Together with the importance of the data being backed up, the quantity of the data, and the frequency of change, the ***[ENTITY]*** should select the most appropriate backup media and backup tools for its purposes. Common backup media include tapes, network drives, and optical media such as Digital Versatile Discs (DVDs).

14.6 ALTERNATIVE STORAGE SITES

Backup media should be stored at alternative locations to enable the restoration of data in the event of an incident at the main processing site. Transportation to and from such alternative sites should be well protected, and only reliable means of transportation should be used.

Note: Due to the requirement of off-site storage for backup data, network drives-mentioned as a backup option in the previous paragraph-are only permitted if they are located at the alternative storage site.

14.7 BACKUP TESTING/RESTORATION

Backup media should be periodically tested to ensure the data contained is still retrievable. A practical solution is to restore from backups when installing a copy of the live system onto the testing environment.

The ***[ENTITY]*** should also monitor its backup media to prevent utilising tapes, discs, and other media past their recommended life spans.

15. OUTLINE DATA CLASSIFICATION PROCEDURE

15.1 OVERVIEW

All ***[ENTITY]*** employees have a responsibility to protect their data from unauthorised access, modification, disclosure, transmission, or destruction. To ensure the confidentiality, integrity, and availability of the ***[ENTITY]***'s data, a data classification framework must be established. All ***[ENTITY]*** employees and contractors working with Abu Dhabi Government data are required to familiarise themselves and comply with this policy.

15.2 DATA CLASSIFICATION

Data Classification is the labelling of data for its most effective and efficient use without compromising its confidentiality, integrity, and availability. Data Owners are responsible for implementing appropriate management and functional controls to govern access to, use of, transmission of, and disposal of Abu Dhabi Government data. It is the System Owner's responsibility to classify data and ensure that it is properly labelled and handled.

Data owned, used, created, or maintained by the Abu Dhabi Government is classified according to the following three categories:

i. Public

ii. For Official Use Only

iii. Confidential

15.3 PUBLIC DATA

Public data is information that may or must be available to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. While subject to Abu Dhabi Government disclosure rules, this data is available to all members of the Government, as well as to residents of the Emirate and the world.

Some examples of public data include:

i. Information posted on the Abu Dhabi e-Government Portal

ii. Government services directory information

15.4 FOR OFFICIAL USE ONLY DATA

For Official Use Only data is information that must be guarded due to proprietary, ethical, or privacy considerations, and protected from unauthorised access, modification, transmission, storage, or other use. This classification applies to data that does not require protection by law or decree, but whose disclosure could negatively impact the operations and/or reputation of the Abu Dhabi Government. This type of information is only accessible to Abu Dhabi Government employees and contractors on a need-to-know basis at the Data Owner's discretion for legitimate business purposes.

Some examples of For Official Use Only data include:

i. Employment data

ii. Information systems documentation

15.5 CONFIDENTIAL DATA

Confidential data is information protected by statutes, regulations, Abu Dhabi Government policies, or contractual language. Confidential data may be disclosed to individuals on a need-to-know basis only, and disclosure to external parties should be authorised by executive management.

Some examples of Confidential data include:

i. Personnel and payroll records

ii. Any data identified by Government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction

The Chief Information Security Officer (CISO) must be notified in a timely manner if data classified as Confidential or For Official Use Only is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed in this manner.

16. OUTLINE ACCEPTABLE USE POLICY

Note: *A sample Acceptable Use Policy (derived from www.sans.org) is provided below. It is recommended that all employees be required to sign it prior to receiving access to the* ***[ENTITY]****'s systems.*

16.1 OVERVIEW

The ***[ENTITY]***'s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the ***[ENTITY]***'s established culture of openness, trust, and integrity. The ***[ENTITY]*** is committed to protecting its employees, partners, and the organisation as a whole from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/intranet/extranet-related systems—including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Web browsing, and FTP-are the property of the ***[ENTITY]***. These systems are to be used for business purposes in serving the interests of the organisation, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every ***[ENTITY]*** employee and affiliate who deals with the service and its supporting systems. It is the responsibility of every computer user to know these guidelines and conduct their activities accordingly.

16.2 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at the ***[ENTITY]***. These rules are in place to protect the employee and the ***[ENTITY]***. Inappropriate use exposes the ***[ENTITY]*** to risks that can include virus attacks, compromise of network systems/services, and legal issues.

16.3 SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at the ***[ENTITY]***, including all personnel affiliated with third parties. It applies to all equipment that is owned or leased by the ***[ENTITY]***.

16.4 POLICY

16.4.1 General Use and Ownership

1. While the ***[ENTITY]***'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on corporate systems remains the property of the ***[ENTITY]***. Because of the need to protect the ***[ENTITY]***'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to the ***[ENTITY]***.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/intranet/extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, to consult their supervisor or manager.
3. For security and network maintenance purposes, authorised individuals within the ***[ENTITY]*** may monitor equipment, systems, and network traffic at any time.

4. The *[ENTITY]* reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

16.4.2 Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorised access to the *[ENTITY]*'s information.
2. Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. End user passwords should be changed *[value as per policy]*.
3. All personal computers, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at *[value as per policy]* minutes or less, or by logging off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use information encryption in compliance with the *[ENTITY]*'s encryption policy.
5. Postings by employees from an *[ENTITY]* e-mail address to newsgroups, discussion boards, and other Web sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the *[ENTITY]* unless the post is made in the course of business duties.
6. All hosts used by the employee that are connected to the *[ENTITY]* Internet/intranet/extranet, whether owned by the employee or the *[ENTITY]*, shall be continually executing approved virus scanning software with a current virus database unless this is overridden by departmental or group policy.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, as these may contain malware such as viruses, e-mail bombs, or Trojan horse code.

16.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the *[ENTITY]* authorised to engage in any activity that is illegal under the law while utilising *[ENTITY]*-owned resources.

The lists below are by no means exhaustive, but are an attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or organisation protected by copyright, trade secret, patent, or other intellectual property, or similar laws and regulations, including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the *[ENTITY]*.
2. Unauthorised copying of: copyrighted material including but not limited to digitisation and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music; and the installation of any copyrighted software for which the *[ENTITY]* or the end user does not have an active license.
3. Purposely introducing malicious programmes into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4. Revealing your account password to others, or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using an ***[ENTITY]*** computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and regulations.
6. Making fraudulent offers of products, items, or services originating from any ***[ENTITY]*** account or system.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties.
8. Port scanning or security scanning, unless prior notification is given to the ***[ENTITY]***'s Chief Information Security Officer (CISO).
9. Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network, or account.
11. Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attacks).
12. Using any programme/script/command, or sending messages of any kind, with the intent to interfere with or disable other users, via any means, locally or via the Internet/intranet/extranet.

E-mail and Communications Activities

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
2. Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of e-mail header information.
4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters," "Ponzi," or other pyramid schemes of any type.
6. Use of unsolicited e-mail originating from the ***[ENTITY]***'s networks of other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by the ***[ENTITY]*** or connected via the ***[ENTITY]***'s network.

16.4.4 Blogging

1. Blogging by employees, whether using the ***[ENTITY]***'s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the ***[ENTITY]***'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the ***[ENTITY]***'s policy, is not detrimental to the ***[ENTITY]***'s best interests, and does not interfere with an employee's regular work duties. Blogging from the ***[ENTITY]***'s systems is also subject to monitoring.
2. The ***[ENTITY]***'s Confidential Information Policy also applies to blogging. As such, employees are prohibited from revealing any confidential or proprietary information, trade secrets, or any other material covered by the ***[ENTITY]***'s Confidential Information Policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of the ***[ENTITY]*** and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by the ***[ENTITY]***'s non-discrimination and anti-harassment policy.
4. Employees shall not attribute personal statements, opinions, or beliefs to the ***[ENTITY]*** when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the ***[ENTITY]***. Employees assume any and all risks associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the ***[ENTITY]***'s trademarks, logos, and any other ***[ENTITY]*** intellectual property shall not be used in connection with any blogging activity.

16.5 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

16.6 DEFINITIONS

Blogging: writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Spam: unauthorised and/or unsolicited electronic mass mailings.

APPENDICES

APPENDIX A: ACRONYMS

ADAA	Abu Dhabi Accountability Authority
ADG-ISO	Abu Dhabi Government – Information Security Office
ADGE	Abu Dhabi Government Entities
ADP	The General Directorate of Abu Dhabi Police
ADSIC	Abu Dhabi Systems & Information Centre
ATO	Authority to Operate
BCM	Business Continuity Management
BCP	Business Continuity Plan
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Certifying Official
CVE	Common Vulnerability Exposure
DAA	Designated Approval Authority
DTO	Denial To Operate
HR	Human Resources
IATO	Interim Authority to Operate
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Protection System
IS	Information Security
ISMS	Information Security Management System
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commission
ISP	Information Security Plan
ISWG	Information Security Working Group
IT	Information Technology
IV&V	Independent Verification and Validation

NIST	National Institute of Standards and Technology
PDCA	Plan-Do-Check-Act
POC	Point Of Contact
ROE	Rules Of Engagement
SQL	Structured Query Language
ST&E	Security Testing and Evaluation
UAE	United Arab Emirates

APPENDIX B: REFERENCES

Abu Dhabi Risk Management Guide, December 2008.

Abu Dhabi Risk Assessment Guide, December 2008.

Abu Dhabi Information Security Planning Guide, December 2008.

Abu Dhabi Security Testing & Evaluation Guide, December 2008.

Abu Dhabi Certification & Accreditation Guide, December 2008.

Abu Dhabi Technical Testing Guide, December 2008.

Abu Dhabi Information Security Policies and Procedures Guide, March 2009.

Information Security Forum, *Standard of Good Practice for Information Security*, 2007.

International Organisation for Standardisation/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005.

International Organisation for Standardisation/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management*, June 2005.

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 188, *Standard Security Labels for Information Transfer*, September 1994.

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 800-53, *Risk Management Guide for Information Technology Systems*, December 2007.

National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology (NIST) Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Standards and Technology (NIST) Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

APPENDIX C: DEFINITIONS

Accreditation	The official management decision given by a senior entity official (chairman) to authorise operation of a Government service and to explicitly accept the risk to entity operations, entity assets, or individuals based on the implementation of an agreed-upon set of security controls
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information
Audit	A formal (independent) review and examination of a project or project activity for assessing compliance with policy and standards
Asset	Anything that has value to the organisation, such as information or information systems
Availability	Ensuring timely and reliable access to and use of information
Certification	Comprehensive assessment of the management and functional security controls in a Government service, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security risk requirements for the services
Certifying Official	Individual, group, or organisation responsible for conducting an information security certification (see definition for Certification)
Confidentiality	Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Control	Means of managing risk, including policies, procedures, guidelines, practices, or organisational structures, which can be of administrative, technical, management, or legal nature
Control Families	Management and functional processes that are grouped into 14 specific families (e.g., Policy and Standards, Human Resources Management, etc.) in order to provide the foundation for a comprehensive Information Security Programme
Control Standards (also referred to as Standards)	Level of security that is deemed necessary (based on international standards and risk assessment) to ensure adequate security. Standards are delineated into two categories: (i) baseline, or the minimum, control standards that must be met for all risk environments; and (ii) enhancements that are recommended for moderate or high risk environments
Cost-Effective Control	A control is determined to be cost effective if the cost of implementing and maintaining the control is economical in in comparison with the risk that it is mitigating

Designated Approval Authority	Individual who has the ultimate responsibility to accredit all Government services. This individual accepts responsibility for the security of the service and accountability for any adverse impacts to the entity if a breach of security occurs
Functional Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems)
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies
Independent Verification & Validation	The process of evaluating work products by a party who is technically, managerially, and financially independent of designing and/or executing the project under review
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms
Information Security	Protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability
Information Security Plan	Formal document that provides an overview of the security requirements for the Government service and describes security controls in place or planned for meeting these requirements
Information System	A discrete set of information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information, including manual processes or automated processes. This includes information systems used by an entity either directly or used by another entity, or a contractor under a contract with the entity that: (i) requires the use of such information systems; or (ii) requires the use, to significant extent, of such information systems in the performance of a service or the furnishing of a product
Information Security Event	Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security-relevant
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information Technology	Any equipment or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information
Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
IT Assets	Computer equipment, such as servers, workstations, routers, firewalls, etc.

Malicious Code	Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of an information system (e.g., virus, worm, Trojan horse, other code-based entity that infects a host). Spyware and some forms of adware are also examples of malicious code
Management Controls	Security controls (i.e., safeguards or countermeasures) for an information system that focuses on the management of risk and the management of information system security.
Mitigation of Risk	Reducing risks to an acceptable level by applying controls
Personally Identifiable Information	Information in an information system: (i) that directly identifies an individual (e.g., name, address, or other identifying number or code, telephone number, email address, etc.), or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors
Policy	Overall intention and direction as formally expressed by management
Potential Impact	The loss of confidentiality, integrity, and/or availability could have (i) low adverse effect; (ii) a moderate adverse effect; or (iii) a high adverse effect on organizational operations, assets, or individuals
Privacy	Information that is linked to a specific individual or group and is controlled and managed by that individual or group – even after that information is willingly shared with a third party – such as to avoid the unwanted disclosure of private information, which could result in damaging effects for the individual. Information Security must include the implementation of controls related to private information. Best practices include the ability to provide the justification and rationalisation for why the use of private information is necessary instead of the use of an alternate identifying schema
Residual Risk	Risk remaining after implementation or enhancement of a control
Risk	The level of impact on entity services, assets, or individuals resulting form the potential consequences of a threat and the likelihood of that threat occurring
Risk Analysis	Systematic use of information to identify sources and to estimate the risk
Risk Assessment	Overall process of risk analysis and risk evaluation
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk Treatment	Process of selecting and implementing controls to modify risk
Spyware	Software that is secretly or surreptitiously installed on an information system to gather information on individuals or organisations without their knowledge. Spyware is a type of malicious code

Standards (also referred to as Control Standards)	Level of security that is deemed necessary (based on international standards and risk assessment) to ensure adequate security. Standards are delineated into two categories: (i) baseline, or the minimum, control standards that must be met for all risk environments; and (ii) enhancements that are recommended for moderate or high risks environments
Third Party	Person or body that is recognised as being independent of the parties involved
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization
Threat Source	Intent and method targeted at the intentional exploitation of vulnerability, or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats