

# **NATIONAL CYBER SECURITY BASELINE**

**Version 1.4**

## REVISION HISTORY

| Version | Revision Date    | Amendment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | 1 October 2024   | Initial Release                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 1.1     | 20 December 2024 | <ul style="list-style-type: none"><li>- Updated the stress test frequency in section 3.4.2.4 to include the clause 'whenever required'.</li><li>- Added Multi-Factor Authentication (MFA) requirement to the Identity and Access Management element under section 3.11.1.1</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1.2     | 3 March 2025     | Updated the cyber security audit requirement in section 3.3.2.3 to remove the specific mention of internal and external auditors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 1.3     | 25 March 2025    | <ul style="list-style-type: none"><li>- Updated section 3.7.1.3 for the integration of DLP logs to be made with a broader range of tools including security information and event monitoring (SIEM), with the purpose of enhancing threat detection, analysis, and incident response capabilities.</li><li>- Updated section 3.10.3.2 and 3.10.3.4 to change from focusing on IPS rules to a broader network threat detection capability.</li><li>- Updated section 3.10.4.2 to expand the integration of logs from malware detection and prevention software to include a broader range of tools including security information and event monitoring (SIEM), for centralised monitoring and correlation of events to detect sophisticated attacks.</li></ul> |

| Version | Revision Date     | Amendment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.4     | 23 September 2025 | <ul style="list-style-type: none"> <li>- Updated section 3.4.2.4 by replacing 'Stress tests shall be performed annually or whenever required to confirm the resilience of the system's performance.' with 'Performance test shall be conducted prior to system go-live or whenever required to validate and confirm the resilience of the system's performance'</li> <li>- Updated section 3.7.4.3 from 'The configuration logs shall be recorded and maintained.' with 'The configuration logs shall be recorded and maintained to support regulatory compliance'.</li> <li>- Replaced 'password management system' with 'password policy' in section 3.11.3.3</li> </ul> |

# TABLE OF CONTENTS

|             |                                                  |           |
|-------------|--------------------------------------------------|-----------|
| <b>1.0</b>  | <b>OVERVIEW.....</b>                             | <b>1</b>  |
| <b>2.0</b>  | <b>BASELINE COMPONENTS.....</b>                  | <b>1</b>  |
| <b>3.0</b>  | <b>CATEGORIES AND ELEMENTS.....</b>              | <b>2</b>  |
| <b>3.1</b>  | <b>CYBER SECURITY POLICY AND OBJECTIVES.....</b> | <b>2</b>  |
| 3.1.1       | Cyber Security Policy .....                      | 2         |
| 3.1.2       | Cyber Security Objectives.....                   | 3         |
| <b>3.2</b>  | <b>ORGANISATIONAL DEVELOPMENT.....</b>           | <b>3</b>  |
| 3.2.1       | Resources (Manpower and Budget).....             | 3         |
| 3.2.2       | Authorities and Special Interest Group.....      | 3         |
| 3.2.3       | Cyber Security Awareness and Training .....      | 4         |
| <b>3.3</b>  | <b>CYBER SECURITY ASSURANCE.....</b>             | <b>4</b>  |
| 3.3.1       | IT Acceptable Use Policy.....                    | 4         |
| 3.3.2       | Cyber Security Audit.....                        | 4         |
| 3.3.3       | Supplier Relationship Security .....             | 5         |
| <b>3.4</b>  | <b>RESOURCE ALLOCATION AND OPTIMISATION.....</b> | <b>5</b>  |
| 3.4.1       | Asset Management .....                           | 5         |
| 3.4.2       | Capacity Management.....                         | 5         |
| <b>3.5</b>  | <b>RISK MANAGEMENT .....</b>                     | <b>6</b>  |
| 3.5.1       | Risk Assessment.....                             | 6         |
| 3.5.2       | Risk Treatment.....                              | 6         |
| <b>3.6</b>  | <b>OPERATIONAL EFFICIENCY.....</b>               | <b>7</b>  |
| 3.6.1       | Change Management .....                          | 7         |
| <b>3.7</b>  | <b>DATA SECURITY.....</b>                        | <b>7</b>  |
| 3.7.1       | Data Leakage Prevention (DLP) .....              | 7         |
| 3.7.2       | Data Privacy and Protection .....                | 7         |
| 3.7.3       | Software and Application Security.....           | 8         |
| 3.7.4       | Secure Configuration.....                        | 8         |
| <b>3.8</b>  | <b>CONTRACTUAL MANAGEMENT.....</b>               | <b>9</b>  |
| 3.8.1       | Non-Disclosure Agreement.....                    | 9         |
| <b>3.9</b>  | <b>PHYSICAL SECURITY.....</b>                    | <b>9</b>  |
| 3.9.1       | Physical Security Procedure.....                 | 9         |
| 3.9.2       | Security Perimeters .....                        | 9         |
| <b>3.10</b> | <b>SYSTEM AND NETWORK SECURITY .....</b>         | <b>10</b> |
| 3.10.1      | Network Security Policies and Procedures.....    | 10        |
| 3.10.2      | Physical and Logical Network Diagrams .....      | 10        |
| 3.10.3      | Network Security Controls .....                  | 11        |
| 3.10.4      | Malware Detection and Prevention.....            | 11        |
| <b>3.11</b> | <b>ACCESS CONTROL .....</b>                      | <b>12</b> |
| 3.11.1      | Identity and Access Management.....              | 12        |
| 3.11.2      | Segregation of Duties.....                       | 12        |
| 3.11.3      | Password Management.....                         | 12        |
| <b>3.12</b> | <b>TECHNICAL VULNERABILITY .....</b>             | <b>13</b> |
| 3.12.1      | Vulnerability Management Procedure .....         | 13        |
| 3.12.2      | Vulnerability Assessment.....                    | 13        |

|             |                                                      |           |
|-------------|------------------------------------------------------|-----------|
| <b>3.13</b> | <b>CYBER SECURITY EVENT MANAGEMENT .....</b>         | <b>14</b> |
| 3.13.1      | Event Management .....                               | 14        |
| <b>3.14</b> | <b>CYBER SECURITY INCIDENT MANAGEMENT .....</b>      | <b>14</b> |
| 3.14.1      | Cyber Security Incident Procedure and Handling ..... | 14        |
| <b>3.15</b> | <b>BUSINESS CONTINUITY MANAGEMENT .....</b>          | <b>14</b> |
| 3.15.1      | Business Continuity Plan .....                       | 14        |
| 3.15.2      | Testing and Simulation .....                         | 15        |
| <b>4.0</b>  | <b>SUMMARY.....</b>                                  | <b>15</b> |
| <b>5.0</b>  | <b>REFERENCES.....</b>                               | <b>15</b> |

## **1.0 OVERVIEW**

National Cyber Security Baseline (NCSB) is a set of minimum security controls and best practices that organisations need to implement and ensure a basic level of cyber security protection.

NCSB encompasses six key domains of cyber security: Govern, Identify, Protect, Detect, Respond, and Recover. These domains span the entire spectrum of cyber security management, from governance and policy oversight to identifying and protecting critical assets, detecting threats, responding to incidents, and ensuring swift recovery.

NCSB is a strategic initiative aimed at fortifying the cyber security defences of organisations across various sectors. This comprehensive baseline serves as a blueprint for organisations to implement and maintain essential security measures, ensuring the protection of critical information assets and systems.

## **2.0 BASELINE COMPONENTS**

The baseline is structured around 15 essential cyber security categories / aspects, which encompass various areas. These categories are further distributed into 33 specific elements, each designed to address distinct aspects of cyber security. All of these are encompassed within six overarching domains.

This structure is designed to enable organisations to manage their cyber security efforts in a layered, structured manner—first identifying broader categories and then implementing the specific elements related to each category. Each element is meticulously crafted to ensure the protection of the organisation's critical information and systems from a wide range of cyber security threats.

Figure 1 illustrates the Cyber Security Baseline Components.

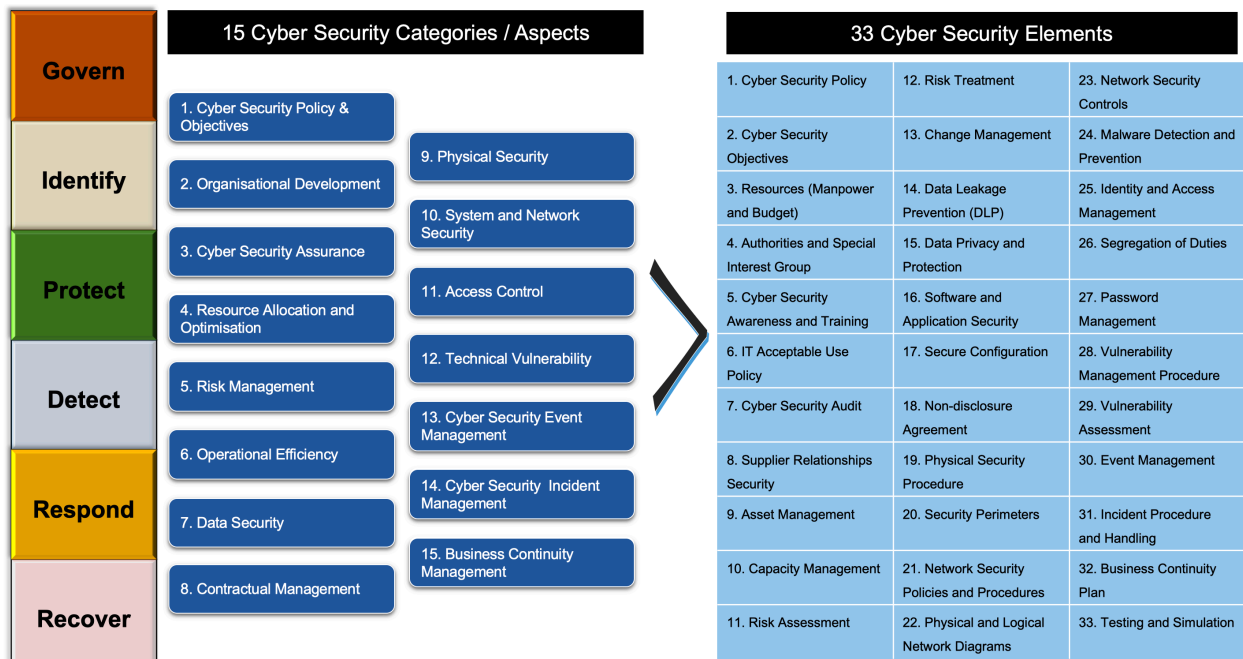


Figure 1: Cyber Security Baseline Components

## 3.0 CATEGORIES AND ELEMENTS

### 3.1 CYBER SECURITY POLICY AND OBJECTIVES

#### 3.1.1 Cyber Security Policy

##### 3.1.1.1 Establishment of the Cyber Security Policy

The organisation shall establish a cyber security policy.

##### 3.1.1.2 Alignment with Best Practices

The cyber security policy shall be aligned with industry best practices.

##### 3.1.1.3 Application of the Cyber Security Policy

The cyber security policy shall be applied across the organisation.

##### 3.1.1.4 Review of the Cyber Security Policy

The cyber security policy shall be reviewed annually and / or when changes are required.

##### 3.1.1.5 Communication

The cyber security policy shall be proactively communicated to all relevant stakeholders.

### **3.1.2 Cyber Security Objectives**

#### **3.1.2.1 Development of Cyber Security Objectives**

The organisation shall develop cyber security objectives that are consistent with its cyber security policy.

#### **3.1.2.2 Communication of Cyber Security Objectives**

The cyber security objectives shall be communicated to relevant stakeholders.

#### **3.1.2.3 Monitoring and Reporting**

The cyber security objectives shall be continuously monitored, tracked and reported annually to the management.

## **3.2 ORGANISATIONAL DEVELOPMENT**

### **3.2.1 Resources (Manpower and Budget)**

#### **3.2.1.1 Definition of Roles and Responsibilities**

The organisation shall define cyber security roles and responsibilities.

#### **3.2.1.2 Communication of Roles and Responsibilities**

The defined cyber security roles and responsibilities shall be communicated to all relevant stakeholders.

#### **3.2.1.3 Allocation of Resources**

Resources shall be allocated by the defined cyber security roles and responsibilities.

#### **3.2.1.4 Review of Resources**

Allocated resources shall be reviewed annually and / or when changes are required.

### **3.2.2 Authorities and Special Interest Group**

#### **3.2.2.1 Establishment of Contacts**

The organisation shall establish contacts with relevant authorities and special interest groups.

#### **3.2.2.2 Communication of Contacts**

The contact information for relevant authorities and special interest groups shall be communicated to the stakeholders.

#### **3.2.2.3 Review of Contacts**

The contact information shall be reviewed annually and / or when changes are required.

### **3.2.3 Cyber Security Awareness and Training**

#### **3.2.3.1 Establishment of Training Plan**

The organisation shall develop and establish a cyber security awareness training plan.

#### **3.2.3.2 Conducting Training Programs**

Cyber security awareness training programs shall be conducted across the organisation.

#### **3.2.3.3 Evaluation of Effectiveness**

The effectiveness of cyber security awareness training programs shall be evaluated upon completion.

## **3.3 CYBER SECURITY ASSURANCE**

### **3.3.1 IT Acceptable Use Policy**

#### **3.3.1.1 Establishment of IT Acceptable Use Policy**

The organisation shall develop and establish an IT acceptable use policy.

#### **3.3.1.2 Application of IT Acceptable Use Policy**

The IT acceptable use policy shall be applied across the organisation.

#### **3.3.1.3 Review of IT Acceptable Use Policy**

The IT acceptable use policy shall be reviewed when changes are required.

### **3.3.2 Cyber Security Audit**

#### **3.3.2.1 Establishment and Approval of Audit Plan**

The organisation shall establish a cyber security audit plan.

#### **3.3.2.2 Approval of Audit Plan**

The cyber security audit plan shall be approved by the management.

#### **3.3.2.3 Conducting the Audit**

Cyber security audits shall be conducted at least biennially by certified auditors.

#### **3.3.2.4 Reporting Findings**

Audit findings shall be reported to the management and relevant stakeholders.

#### **3.3.2.5 Resolution of Non-Compliance**

Any non-compliances identified during the audit shall be resolved in a timely manner and reported to the management and relevant stakeholders.

### **3.3.3 Supplier Relationship Security**

#### **3.3.3.1 Establishment of Supply Chain Management Policy**

The organisation shall define a supply chain management policy.

#### **3.3.3.2 Identification and Documentation of External Service Providers**

External service providers shall be identified and documented.

#### **3.3.3.3 Review of Supply Chain Management Policy**

The supply chain management policy and the list of external providers shall be reviewed annually.

## **3.4 RESOURCE ALLOCATION AND OPTIMISATION**

### **3.4.1 Asset Management**

#### **3.4.1.1 Establishment of IT Assets Inventory**

The organisation shall establish an IT assets inventory.

#### **3.4.1.2 Maintenance of IT Assets Inventory**

The IT assets inventory shall be maintained.

#### **3.4.1.3 Classification and Ownership**

The IT assets shall be classified and assigned to the appropriate ownership.

#### **3.4.1.4 Review of IT Assets Inventory**

The IT assets inventory shall be reviewed annually and/ or when changes are required.

### **3.4.2 Capacity Management**

#### **3.4.2.1 Establishment of Capacity Management Plan**

The organisation shall establish a capacity management plan.

#### **3.4.2.2 Tracking and Monitoring Resource Utilisation**

Resource utilisation shall be tracked and monitored.

- 3.4.2.3 Review and Forecasting**  
Resource utilisation results shall be reviewed annually and the necessary resource forecasts shall be taken.
- 3.4.2.4 Performance Tests**  
Performance test shall be conducted prior to system go-live or whenever required to validate and confirm the resilience of the system's performance.

## **3.5 RISK MANAGEMENT**

### **3.5.1 Risk Assessment**

- 3.5.1.1 Establishment of Risk Assessment Process**  
The organisation shall establish cyber security risk assessment process.
- 3.5.1.2 Alignment with Best Practices**  
The cyber security risk assessment process shall be aligned with best practices.
- 3.5.1.3 Conducting Assessments**  
The cyber security risk assessments shall be conducted annually and / or when changes are required.
- 3.5.1.4 Documentation and Reporting**  
The results of the cyber security risk assessment shall be documented and reported to the management and / or relevant stakeholders.
- 3.5.1.5 Risk Prioritization**  
The identified risks shall be prioritized for treatment.

### **3.5.2 Risk Treatment**

- 3.5.2.1 Formulation of Risk Treatment Plan**  
The organisation shall formulate a risk treatment plan.
- 3.5.2.2 Approval of Plan**  
The risk treatment plan shall be approved by the risk owner or the management.
- 3.5.2.3 Implementation of Plan**  
The approved risk treatment plan shall be implemented.
- 3.5.2.4 Documentation and Reporting**  
The results of the risk treatment shall be documented and reported to the management and / or relevant stakeholders.

## **3.6 OPERATIONAL EFFICIENCY**

### **3.6.1 Change Management**

#### **3.6.1.1 Establishment of Change Management Procedure**

The organisation shall establish a change management procedure for managing changes to information processing facilities, information systems, and other relevant components.

#### **3.6.1.2 Application of Change Management Procedure**

The change management procedure shall be applied across the organisation.

#### **3.6.1.3 Authorisation for Changes**

Authorisation must be obtained before implementing any changes to information processing facilities, information systems, or other relevant components.

#### **3.6.1.4 Review of Change Management Procedure**

The change management procedure shall be reviewed annually and / or when changes are required.

## **3.7 DATA SECURITY**

### **3.7.1 Data Leakage Prevention (DLP)**

#### **3.7.1.1 Implementation of DLP Solution**

The organisation shall apply data leakage prevention (DLP) solution across the organisation.

#### **3.7.1.2 Maintenance of DLP Solution**

The DLP solution shall be maintained regularly.

#### **3.7.1.3 Integration with Security Monitoring Tools**

The DLP logs shall be integrated with tools such as security information and event monitoring (SIEM), that enhance threat detection, analysis and incident response capabilities.

### **3.7.2 Data Privacy and Protection**

#### **3.7.2.1 Establishment of Data Privacy and Protection Procedure**

The organisation shall define data privacy and protection procedure.

#### **3.7.2.2 Alignment with Legal and Regulatory Requirements**

The data privacy and protection procedure shall be aligned with legal and regulatory requirements.

**3.7.2.3 Application of Data Privacy and Protection Procedure**  
The data privacy and protection procedure shall be applied across the organisation.

**3.7.2.4 Monitoring Compliance**  
Compliance with the data privacy and protection procedure shall be regularly monitored.

**3.7.2.5 Review of Data Privacy and Protection Procedure**  
The data privacy and protection procedure shall be reviewed annually and / or when changes are required.

### **3.7.3 Software and Application Security**

**3.7.3.1 Establishment of Guidelines**  
The organisation shall establish cyber security guidelines for software and system / applications development.

**3.7.3.2 Implementation of Guidelines**  
The cyber security for guidelines software and system / applications development is implemented.

**3.7.3.3 Requirement Identification, Specification and Approval**  
The cyber security requirements shall be identified, specified and approved by the management when developing software and system / applications.

**3.7.3.4 Security Testing**  
The organisation shall conduct security testing on software and system / applications before their deployment in a production environment.

### **3.7.4 Secure Configuration**

**3.7.4.1 Establishment of Configuration Procedures**  
The organisation shall establish procedures for the configuration of hardware, software, services, and networks.

**3.7.4.2 Monitoring and Approval**  
The configuration shall be monitored and reviewed regularly and any updates or installations shall be based on the management's approval.

**3.7.4.3 Logs**  
The configuration logs shall be recorded and maintained to support regulatory compliance.

## **3.8 CONTRACTUAL MANAGEMENT**

### **3.8.1 Non-Disclosure Agreement**

#### **3.8.1.1 Establishment of Non-Disclosure Agreements**

The organisation shall establish an NDAs (non-disclosure agreements).

#### **3.8.1.2 Signing of Non-Disclosure Agreements**

The NDAs shall be signed by all relevant parties.

#### **3.8.1.3 Monitoring and Reporting Compliance**

The organisation shall monitor compliance with the signed NDAs and any instances of non-compliance shall be reported to the management.

## **3.9 PHYSICAL SECURITY**

### **3.9.1 Physical Security Procedure**

#### **3.9.1.1 Establishment of Physical Security Procedure**

The organisation shall establish a physical security procedure.

#### **3.9.1.2 Alignment with Best Practices**

The physical security procedure shall be aligned with best practices.

#### **3.9.1.3 Application of Physical Security Procedure**

The physical security procedure shall be applied across the organisation.

#### **3.9.1.4 Monitoring Compliance**

Compliance with the physical security procedure shall be regularly monitored.

#### **3.9.1.5 Review of Physical Security Procedure**

The physical security procedure shall be reviewed annually and / or when changes are required.

### **3.9.2 Security Perimeters**

#### **3.9.2.1 Establishment of Security Perimeters**

The organisation shall establish security perimeters to prevent unauthorised physical access, damage and interference to the organisation's information.

- 3.9.2.2 Monitoring**  
The organisation shall continuously monitor the premise to prevent unauthorised physical access.
- 3.9.2.3 Protection Against Threats**  
The organisation shall design and implement protections against physical and environmental threats to reduce the consequences of unwanted events.

### **3.10 SYSTEM AND NETWORK SECURITY**

#### **3.10.1 Network Security Policies and Procedures**

- 3.10.1.1 Establishment of Network Security Policy and Procedure**  
The organisation shall establish network security policy and procedure.
- 3.10.1.2 Management Approval**  
The network security policy and procedure shall be approved by the management.
- 3.10.1.3 Alignment with Industry Best Practices**  
The network security policy and procedure shall be aligned with industry best practices.
- 3.10.1.4 Monitoring Compliance**  
Compliance with the network security policy and procedure shall be regularly monitored.
- 3.10.1.5 Review of Network Security Policy and Procedure**  
The network security policy and procedure shall be reviewed annually and / or when changes are required.

#### **3.10.2 Physical and Logical Network Diagrams**

- 3.10.2.1 Establishment of Physical and Logical Network Diagrams**  
The organisation shall define the physical and logical network diagrams.
- 3.10.2.2 Alignment with Best Practices**  
The network diagrams shall be aligned with best practices.
- 3.10.2.3 Inclusion of Advanced Security Controls**  
The network diagrams shall consist of advanced security controls such as next-generation firewalls (NGFW) , intrusion detection and prevention systems (IDPS),

security information and event management (SIEM) systems, and zero trust architecture.

- 3.10.2.4 Review of Physical and Logical Network Diagrams**  
The network diagrams shall be reviewed when changes are required.

### **3.10.3 Network Security Controls**

- 3.10.3.1 Firewall Rules Implementation**  
The organisation shall implement firewall rules to control traffic between the network segments.
- 3.10.3.2 Network Threat and Detection Capability**  
The organisation shall implement network threat and detection capability to enable early detection and response to suspicious network activities.
- 3.10.3.3 Network Access Control (NAC) Solutions**  
The organisation shall implement NAC solutions across the organisation to enforce access policies.
- 3.10.3.4 Review of Network Security Control**  
The organisation shall review the firewall rules, network threat detection capability, and NAC solutions annually and / or when changes are required.

### **3.10.4 Malware Detection and Prevention**

- 3.10.4.1 Implementation of Malware Detection and Prevention Software**  
The organisation shall implement malware detection and prevention software.
- 3.10.4.2 Integration with Security Monitoring Tools**  
Logs from the malware detection and prevention software shall be integrated with tools such as security information and event monitoring (SIEM), that enable centralized monitoring and correlation of events to detect sophisticated attacks.
- 3.10.4.3 Regular Analysis and Evaluation**  
Logs from the malware detection and prevention software shall be regularly analysed and evaluated.

## **3.11 ACCESS CONTROL**

### **3.11.1 Identity and Access Management**

#### **3.11.1.1 Establishment of Identity and Access Management Procedures**

The organisation shall establish identity and access management procedure that incorporates Multi-Factor Authentication (MFA).

#### **3.11.1.2 Management Approval**

The identity and access management procedure shall be approved by the management.

#### **3.11.1.3 Monitoring Compliance**

Compliance with the identity and access management procedure including the provision, revocation, and modification of identities shall be regularly monitored.

#### **3.11.1.4 Review of Identity and Access Management Procedures**

The identity and access management procedure shall be reviewed annually and / or when changes are required.

### **3.11.2 Segregation of Duties**

#### **3.11.2.1 Segregation of Duties and Responsibilities**

The organisation shall segregate the duties and responsibilities of employees based on their roles.

#### **3.11.2.2 Defined Roles and Provision**

Roles shall be defined and provisioned to minimise access problems in the event of role removal or reassigned.

#### **3.11.2.3 Review of Duties and Responsibilities**

The segregation of duties of employees shall be reviewed annually and / or when changes are required.

### **3.11.3 Password Management**

#### **3.11.3.1 Establishment of Password Management System**

The organisation shall establish a password management system.

#### **3.11.3.2 Alignment with Best Practices**

The password management system shall be aligned with best practices.

#### **3.11.3.3 Compliance Monitoring**

Compliance with the password policy shall be regularly monitored.

- 3.11.3.4 Review of Password Management System**  
The password management system shall be reviewed annually and / or when changes are required.

## **3.12 TECHNICAL VULNERABILITY**

### **3.12.1 Vulnerability Management Procedure**

- 3.12.1.1 Establishment of Vulnerability Management Procedure**  
The organisation shall establish a vulnerability management procedure.
- 3.12.1.2 Alignment with Best Practices**  
The vulnerability management procedure shall be aligned with best practices.
- 3.12.1.3 Compliance Monitoring**  
Compliance with the vulnerability management procedure shall be regularly monitored.
- 3.12.1.4 Review and Updates**  
The vulnerability management procedure shall be reviewed annually and / or when changes are required.

### **3.12.2 Vulnerability Assessment**

- 3.12.2.1 Establishment of Vulnerability Assessment Plan**  
The organisation shall establish a vulnerability assessment plan.
- 3.12.2.2 Conducting Vulnerability Assessment Plan**  
Vulnerability assessments shall be conducted as per the established plan.
- 3.12.2.3 Monitor and Track**  
The identified vulnerabilities shall be monitored and tracked.
- 3.12.2.4 Evaluate**  
Identified vulnerabilities shall be evaluated and appropriate measures shall be taken to address the vulnerabilities.
- 3.12.2.5 Review and Reporting**  
The outcomes of vulnerability assessments and remediation shall be reviewed and reported to the relevant stakeholders.

### **3.13 CYBER SECURITY EVENT MANAGEMENT**

#### **3.13.1 Event Management**

- 3.13.1.1 Establishment of Security Monitoring Procedure**  
The organisation shall establish a security monitoring procedure.
- 3.13.1.2 Compliance Monitoring**  
Compliance with the security monitoring procedure shall be regularly monitored.
- 3.13.1.3 Review of Security Monitoring Procedure**  
The security monitoring procedure shall be reviewed annually and / or when changes are required.

### **3.14 CYBER SECURITY INCIDENT MANAGEMENT**

#### **3.14.1 Cyber Security Incident Procedure and Handling**

- 3.14.1.1 Establishment of Cyber Security Incident Management Procedure**  
The organisation shall establish a cyber security incident management procedure.
- 3.14.1.2 Response and Handling**  
Cyber security incidents shall be responded to and handled accordingly based on established incident management procedure.
- 3.14.1.3 Review of Cyber Security Incident Management Procedure**  
The cyber security incident management procedure shall be reviewed annually and / or when changes are required.

### **3.15 BUSINESS CONTINUITY MANAGEMENT**

#### **3.15.1 Business Continuity Plan**

- 3.15.1.1 Establishment of Business Continuity Plan**  
The organisation shall establish a business continuity plan.
- 3.15.1.2 Compliance Monitoring**  
Compliance with the business continuity plan shall be regularly monitored.

#### **3.15.1.3**

#### **Review of Business Continuity Plan**

The business continuity plan shall be reviewed annually and / or when changes are required.

### **3.15.2 Testing and Simulation**

#### **3.15.2.1**

#### **Conducting Scenario-Based Testing and Simulations**

The organisation shall conduct scenario-based testing and simulation exercises on an annual basis or when required by the management.

## **4.0 SUMMARY**

The National Cyber Security Baseline (NCSB) is a comprehensive approach to guide organisations in establishing effective cyber security practices. It organises essential security measures into 6 domains, 15 categories and 33 elements, covering areas such as cyber security policy, organisational development, risk management, data security, and incident management. The baseline emphasizes the need for alignment with industry standards and best practices, ensuring that organisations adopt a structured approach to protect their critical information and systems. Through this approach, the NCSB aims to strengthen the overall cyber security posture of the organisations and systematically address various cyber security threats.

## **5.0 REFERENCES**

- i. National Institute for Standards and Technology (NIST). 2024. The NIST Cyber Security Framework (CFS) 2.0.
- ii. ISO/IEC 27001. 2022. Information Security, cybersecurity and privacy protection - Information Security Management Systems – Requirements.
- iii. ISO/IEC 27002. 2022. Information Security, cybersecurity and privacy protection - Information Security Controls