This document has been written in accordance with the ISO 27001 standard. The policies, procedures and forms included in this manual are to be adopted by all employee of [Your Business Name]
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Scope of the Manual</td>
<td>8</td>
</tr>
<tr>
<td>Terms and Definitions</td>
<td>10</td>
</tr>
<tr>
<td>Normative References</td>
<td>11</td>
</tr>
<tr>
<td>Understanding the Organisation and its Context</td>
<td>13</td>
</tr>
<tr>
<td>Understanding the Needs and Expectations of Interested Parties</td>
<td>15</td>
</tr>
<tr>
<td>Determining the Scope of the Information Security Management System</td>
<td>17</td>
</tr>
<tr>
<td>List of Legal, Regulatory, Contractual and other Requirements</td>
<td>18</td>
</tr>
<tr>
<td>Information Security Management System</td>
<td>19</td>
</tr>
<tr>
<td>Leadership and Commitment</td>
<td>21</td>
</tr>
<tr>
<td>Policy</td>
<td>22</td>
</tr>
<tr>
<td>Definition of Security Roles and Responsibilities</td>
<td>24</td>
</tr>
<tr>
<td>Organisation Roles, Responsibilities and Authorities</td>
<td>26</td>
</tr>
<tr>
<td>Actions to Address Risks and Opportunities</td>
<td>28</td>
</tr>
<tr>
<td>Information Security Objectives and Planning to Achieve Them</td>
<td>30</td>
</tr>
<tr>
<td>Resources</td>
<td>31</td>
</tr>
<tr>
<td>Competence</td>
<td>32</td>
</tr>
<tr>
<td>Awareness</td>
<td>33</td>
</tr>
<tr>
<td>Communication</td>
<td>34</td>
</tr>
<tr>
<td>Documented Information</td>
<td>36</td>
</tr>
<tr>
<td>Operation Planning and Control</td>
<td>38</td>
</tr>
<tr>
<td>Information Security Risk Assessment</td>
<td>40</td>
</tr>
<tr>
<td>Information Security Risk Treatment</td>
<td>42</td>
</tr>
<tr>
<td>Risk Treatment Plan</td>
<td>44</td>
</tr>
<tr>
<td>Monitoring, Measurement and Evaluation</td>
<td>45</td>
</tr>
<tr>
<td>Continual Improvement</td>
<td>46</td>
</tr>
<tr>
<td>Internal Audits</td>
<td>48</td>
</tr>
<tr>
<td>Internal Audit - Procedure</td>
<td>50</td>
</tr>
<tr>
<td>Internal Audit - Planning</td>
<td>51</td>
</tr>
<tr>
<td>Internal Audit - Schedule</td>
<td>52</td>
</tr>
<tr>
<td>Internal Audit – Checklist for ISO 27001:2013</td>
<td>53</td>
</tr>
<tr>
<td>Non-Compliance &amp; Disciplinary Process</td>
<td>54</td>
</tr>
<tr>
<td>Management Review</td>
<td>55</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Statement of Applicability</td>
<td>56</td>
</tr>
<tr>
<td>Acceptable Use Policy</td>
<td>57</td>
</tr>
<tr>
<td>Asset Management</td>
<td>58</td>
</tr>
<tr>
<td>Asset Register</td>
<td>62</td>
</tr>
<tr>
<td>Breach Management</td>
<td>64</td>
</tr>
<tr>
<td>- Business Continuity Plan</td>
<td>69</td>
</tr>
<tr>
<td>- Initial Notice</td>
<td>74</td>
</tr>
<tr>
<td>- Responsibilities</td>
<td>77</td>
</tr>
<tr>
<td>Incident Checklist (Evacuation and Non-Evacuation)</td>
<td>80</td>
</tr>
<tr>
<td>Incident Impact Risk Analysis</td>
<td>81</td>
</tr>
<tr>
<td>Business Impact Checklist</td>
<td>83</td>
</tr>
<tr>
<td>Change Management</td>
<td>88</td>
</tr>
<tr>
<td>Data &amp; Backups</td>
<td>90</td>
</tr>
<tr>
<td>Decommissioning and Destruction of Assets</td>
<td>92</td>
</tr>
<tr>
<td>Information Classification Scheme</td>
<td>94</td>
</tr>
<tr>
<td>Information Security Incident Report</td>
<td>95</td>
</tr>
<tr>
<td>Internal/External Communications Plan</td>
<td>97</td>
</tr>
<tr>
<td>Legal Compliance</td>
<td>99</td>
</tr>
<tr>
<td>List of Threats &amp; Vulnerabilities</td>
<td>103</td>
</tr>
<tr>
<td>Management Review Meeting Minutes</td>
<td>105</td>
</tr>
<tr>
<td>Mobile, BYOD and Other Device</td>
<td>107</td>
</tr>
<tr>
<td>Non-Conformance Report</td>
<td>110</td>
</tr>
<tr>
<td>Patch Management</td>
<td>114</td>
</tr>
<tr>
<td>Procedure for Identification of Requirements</td>
<td>116</td>
</tr>
<tr>
<td>Process and Access of Critical or Sensitive Information (Before Collection)</td>
<td>120</td>
</tr>
<tr>
<td>Process and Access of Critical or Sensitive Information (After Collection)</td>
<td>126</td>
</tr>
<tr>
<td>Recording Actions/Events and Intrusion Prevention</td>
<td>128</td>
</tr>
<tr>
<td>- Risk Assessment and Treatment Methodology</td>
<td>133</td>
</tr>
<tr>
<td>- Risk Management Categorisation</td>
<td>138</td>
</tr>
<tr>
<td>- Risk Treatment Plan</td>
<td>140</td>
</tr>
<tr>
<td>- Risk Register</td>
<td>145</td>
</tr>
<tr>
<td>- Risk Treatment Table</td>
<td>149</td>
</tr>
<tr>
<td>Supplier Evaluation Checklist</td>
<td>152</td>
</tr>
<tr>
<td>Termination, Onboarding &amp; Change of Status</td>
<td>155</td>
</tr>
<tr>
<td>Training Register</td>
<td>159</td>
</tr>
</tbody>
</table>

[Date]
Vendor and Third-Party Risk Management
Scope of the Manual

Description
Your Company Name has been operating since (STATE YEAR OF COMMENCEMENT) and is engaged in the business of:

(STATE YOUR MAIN ACTIVITY OR BUSINESS)

This document details the steps and processes that Your Company Name have implemented meet its Information Security Management System (ISMS) objectives and meets the requirements of ISO 27001:2013, the international standard for Information Security Management.

Purpose and Scope
The purpose and objective of this document is to clearly define the boundaries of the Information Security Management System (ISMS). The Information Security Policy is to set out a framework for the protection of the organisation's information assets:

- To protect the organisation's information from all threats, whether internal or external, deliberate or accidental,
- To enable secure information sharing,
- To encourage consistent and professional use of information,
- To ensure that everyone is clear about their roles in using and protecting information,
- To ensure business continuity and minimise business damage,
- To protect the organisation from legal liability and the inappropriate use of information

It is the policy of the organisation to ensure:

- Confidentiality: so that information is accessible only to authorised individuals.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: that authorised users have access to relevant information when required.
- Information is protected from unauthorised access, disclosure, modification or loss.
- Information is authentic.
- Information and equipment are protected from accidental or malicious damage.

This document is applied to all documentation and activities within the ISMS.

Users of this document are members of Your Company Name management, members of the project team implementing the ISMS, and other relevant parties within the organisation.

Definition of ISMS Scope
Your Company Name needs to define the boundaries of its ISMS in order to decide which information it wants to protect. Such information will need to be protected no matter whether it is additionally stored, processed or transferred in or out of the ISMS scope. The fact that some information is available outside of the scope doesn't mean the security measures won't apply to it – this only means that the responsibility for applying the security measures will be transferred to a third party who manages that information.

Taking into account the legal, regulatory, contractual and other requirements, the ISMS scope is defined as specified in the following items:

Processes and Services:
The ISMS covers all normal business activities relating to the provision of:

(STATE YOUR BUSINESS ACTIVITIES COVERED UNDER THE ISMS)
Geographical:
The ISMS covers all administration offices and operations in:

(STATE YOUR AREAS OF OPERATION)

Exclusions:
The ISMS does NOT include the operations of:

(STATE ANY EXCLUSIONS HERE)

Upon the implementation of this manual, upload into the MAUS Hub’s Policy Manager, all version control and tracking will be managed within the MAUS Hub’s internal mechanisms and all relevant records will be managed through this platform.

Policy & Procedure
The ISMS Manual is applicable to all aspects that Your Company Name has identified as those which it can control and those which it can influence.

This manual is a “controlled” document, however “uncontrolled” copies can be distributed to any interested party.

The ISMS Manual is intended to be used as a public document to demonstrate the organisation’s commitment to demonstrating best practice for information security processes.

Application of Policy:
- Speech, spoken face to face, or communicated by phone or radio,
- Hard copy data printed or written on paper,
- Information stored in manual filing systems,
- Communications sent by post / courier, fax, electronic mail,
- Stored and processed via servers, PCs, laptops, mobile phones, PDAs,
- Stored on any type of removable media, CDs, DVDs, tape, USB memory sticks, digital cameras.

This policy is intended to be reviewed on a regular basis to ensure that the policy standards, directives, procedures, incident management and security awareness education are up to date and implemented in an effective fashion. Any amendments to the policy will be implemented within the processes and procedures of the business, as well as implemented within the operational procedures and contractual arrangements present within the business.

Reference Documents
- List of legal, regulatory, contractual and other requirements.
Definition of Security Roles and Responsibilities

Description
Your Company Name has guidelines for all employees regarding security roles and responsibilities.

Purpose & Scope
The purpose of this policy is to explain the general procedures relating to security roles and responsibilities.

The following guidelines are to be adhered to by all employers, supervisors and employees.

Policy & Procedure
Listed below are the roles created by Your Company Name for the design, operation development, audit and measurement of effective ISMS. The responsibilities are included but not limited to:

Senior Management:
Senior management shall demonstrate leadership and commitment with respect to the ISMS by:

- Ensuring the ISMS and the objectives are established and are compatible with the strategic direction of MAUS Business Systems
- Ensuring the integration of the ISMS requirements into MAUS Business Systems’ processes
- Ensuring that the resources needed for the ISMS are available

Authority:
- To take financial decisions on issues related to risk
- Provide prioritisation of risk based on time, impact and probability factors
- Allocation of responsibilities

Data Protection Officer/Chief Information Security Officer (ISO)/ISMS Manager:

Primary Responsibility:
- Maintains and updates an ISMS (or delegates and reviews these duties based on the relevant hierarchy) to keep track or organisational weakness and present to the management for decisions. Decisions requiring implementation are tracked with the relevant implementation team till closure. Vulnerabilities for which there are no action taken are reported for residual risk approval to the senior management.
- Enterprise project or program office – Verifies and performs risk assessment for any new product/project/customer acquisition/other event
- Document Controller for all ISMS related documentation. Document owner is a separate role, CISO is not necessary the document owner for all security policy/procedures, some of which are owned by other departments such as IT, HR. Operations, legal, physical security, application development and top management.

Coordination Responsibility:
- Ensures policy objectives are met and responsible for supervision of records generated as per the security operation
- Information Security budget preparation and submission to senior management for approval
- ISMS program maintenance
- Training & Awareness

Authority:
- To create additional policy, procedure and metrics with respect to ISMS operation, maintenance, implementation or remediation.
- Scheduling mandatory compliance checks

Head of Departments/Product Managers/Team Leaders:
These individuals are responsible to ensure the following processes:
• Understand and owns security/compliance responsibility as distinctive from operational/revenue generating responsibilities
• Their position as Risk Owner for relevant risks: Each department head or other similar figure is owner of risks that are allocated to them in relevance to their jurisdiction. In ISO 270001 this is distributed by the controls to the respective owner, from a formal document – Statement of Applicability
• Encourages team members to report security weaknesses or incidents relevant to any part of the organisation

Authority:
• To inform management about any new risk/vulnerability
• Assist with the implementation of policies, performing of assessments, audits and remediation in relevance to their jurisdiction

ISMS End Users:
• Includes employees without departmental/supervisor responsibilities
• Complies to end-user policy/procedure, namely Acceptable Usage Policy, which provides description of each user behaviour with respect to information usage
• Reports security weakness/incidents to either the head of department or the ISMS security manager.
• End Users do not exploit known security weaknesses.

Authority:
• To report any new weaknesses/incidents to the head of department/data protection officer/CEO

Internal Auditors:
• Functions upon the directives of the senior management/Security forum and carries out regular review of ISMS, based on the defined scope.
• The individuals nominated should be impartial, who has no material benefit in the outcome of Internal audit, positive or negative.
• Makes judgment on the effectiveness of the selected policies, procedures and records
• Individuals will be named on an as needs basis in accordance to their impartibility and availability

Authority:
• To raise non-conformity in any aspect of ISMS operation
Risk Treatment Plan

Description
Your Company Name has guidelines for all employees regarding the Risk Treatment Plan.

Purpose & Scope
The purpose of this policy is to explain the general procedures relating to the risk treatment plan.

The following guidelines are to be adhered to by all employers, supervisors and employees.

Policy & Procedure
In order to achieve the ISMS objectives, the following activities need to be done:

<table>
<thead>
<tr>
<th>Definition of hazard</th>
<th>Description of activities</th>
<th>Necessary financial and other resources</th>
<th>Responsible person</th>
<th>Start and completion deadlines</th>
<th>Training and awareness programs</th>
<th>Method for evaluation of results</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Management Review

Description
Your Company Name has guidelines for all employees regarding management reviews.

Purpose & Scope
The purpose of this policy is to explain the general procedures relating to management reviews.

The following guidelines are to be adhered to by all employers, supervisors and employees.

Policy & Procedure
Your Company Name will evaluate the information security performance and the effectives of the information security management system.

Your Company Name shall determine:

- What needs to be monitored and measured, including information security processes and controls
- The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results.
- When the monitoring and measuring shall be performed
- Who shall monitor and measure?
- When the results form monitoring

Management of Your Company Name will review the organisations ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review will include consideration of:

- The status of actions from previous management reviews
- Changes in external and internal issues that are relevant to the ISMS
- Feedback on the information security performance, including trends in:
  - Nonconformities and corrective actions
  - Monitoring and measurement results
  - Audit results
  - Fulfilment of information security objectives
- Feedback from interested parties
- Results of risk assessment and status of risk treatment plan
- Opportunities for continual improvement

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the ISMS. These will be retained as evidence as outlined by clause 9.3 under ISO 27001:2013.
List of Threats & Vulnerabilities

Description
Your Company Name has guidelines for all employees regarding the list of threats & vulnerabilities. MAUS’ policies and procedures as outlined in this document will address these threats or will identify the areas where the company will be taking ongoing steps to minimise these threats. While we will always be vigilant and ensure that our applications & systems are designed from the ground up to address these threats and our security protocols, monitoring systems & detection tools are reviewed on a consistent basis, the following threats have been identified.

Purpose & Scope
The purpose of this policy is to explain and outline any relevant threats and vulnerabilities to the organisation. This is not a definitive list.

The following guidelines are to be adhered to by all employers, supervisors and employees.

Policy & Procedure
Your Company Name has identified the below possible threats to the business. The company has assessed the below areas based on severity, likelihood and impact and dealt with these individually. The company for all specific identified threats under the heading Specific Identified Threats Your Company Name will establish and maintain up-to-date listings of all the legislations and other regulations relevant to Your Company Name.

The below includes some examples of Threats & Vulnerabilities from the ISO 27001:2013 Framework, this list is not exhaustive:

Threats:

- Access to the network by unauthorised persons
- Bomb attack
- Bomb threat
- Breach of contractual relations
- Breach of legislation
- Compromising confidential information
- Concealing user identity
- Damage caused by a third party
- Damages resulting from penetration testing
- Destruction of records
- Disaster (human caused)
- Disaster (natural)
- Disclosure of information
- Disclosure of passwords
- Eavesdropping
- Embezzlement
- Errors in maintenance
- Failure of communication links
- Falsification of records
- Fire
• Flood
• Fraud
• Industrial espionage
• Information leakage
• Interruption of business processes
• Loss of electricity
• Loss of support services
• Malfunction of equipment
• Malicious code
• Misuse of information systems
• Misuse of audit tools
• Pollution
• Social engineering
• Software errors
• Strike
• Terrorist attacks
• Theft
• Thunderstroke
• Unintentional change of data in an information system
• Unauthorised access to the information system
• Unauthorised changes of records
• Unauthorised installation of software
• Unauthorised physical access
• Unauthorised use of copyright material
• Unauthorised use of software
• User error
• Vandalism

Vulnerabilities:
• Complicated user interface
• Default passwords not changed
• Disposal of storage media without deleting data
• Equipment sensitivity to changes in voltage
• Equipment sensitivity to moisture and contaminants
• Equipment sensitivity to temperature
• Inadequate cabling security
• Inadequate capacity management
• Inadequate change management
• Inadequate classification of information
• Inadequate control of physical access
• Inadequate maintenance
• Inadequate network management
• Inadequate or irregular backup
• Inadequate password management
• Inadequate physical protection
• Inadequate protection of cryptographic keys
• Inadequate replacement of older equipment
• Inadequate security awareness
• Inadequate segregation of duties
• Inadequate segregation of operational and testing facilities
• Inadequate supervision of employees
• Inadequate supervision of vendors
• Inadequate training of employees
• Incomplete specification for software development
• Insufficient software testing
• Lack of access control policy
• Lack of clean desk and clear screen policy
• Lack of control over the input and output data
• Lack of internal documentation
• Lack of or poor implementation of internal audit
• Lack of policy for the use of cryptography
• Lack of procedure for removing access rights upon termination of employment
• Lack of protection for mobile equipment
• Lack of redundancy
• Lack of systems for identification and authentication
• Lack of validation of the processed data
• Location vulnerable to flooding
• Poor selection of test data
• Single copy
• Too much power in one person
• Uncontrolled copying of data
• Uncontrolled download from the Internet
• Uncontrolled use of information systems
• Undocumented software
• Unmotivated employees
• Unprotected public network connections
• User rights are not reviewed regularly

Specific Identified Threats:
(This list is not exhaustive and should be edited and updated in accordance with changes to internal systems and processes):

Threat 1: Masquerading of user identity by insiders: The threat of masquerading of user identity by insiders covers attempts by authorised users to gain access to information to which they have not been granted
access. These users may attempt to gain access to that information by using another user’s account or login credentials.

Threat 2: Masquerading of user identity by contracted service Providers: The threat of masquerading of a user identity by contracted service providers covers attempts by people working for a contracted service provider to obtain unauthorised access to information by using an authorised person.

Threat 3: Masquerading of user identity by outsiders: The threat of masquerading of a user identity by outsiders covers attempts by outsiders to obtain unauthorised access to information by posing as an authorised user.

Threat 4: Unauthorised use of an application: Various cases of unauthorised use of an application.

Threat 5: Introduction of damaging or disruptive software: This threat covers Viruses, Worms, Trojan Horses, logic bombs, any other form of malicious software which could impact the services of our product/s.

Threat 6: Misuse of system resources: Identifies factors that increase the threat of misuse of system resources; covers People playing games on business systems, People using business systems for personal work, People downloading non-work-related information from the internet, People setting up databases or other packages for non-work related matters.

Threat 7: Communications infiltration: This threat covers the following types of event: Hacking into a system using, for example, buffer overflow attacks, masquerading as a server, masquerading as an existing user of an ecommerce application, masquerading as a new user of an ecommerce application, Denial of service (deliberate), Flaming attacks, and Spamming.

Threat 8: Communications interception: This threat covers Passive interception and Traffic monitoring. The ease of interception is determined by two basic factors: The medium of transmission and the type of protocols being used. Interception of some types of traffic on the internet is relatively easy. It can be achieved by attackers sending messages to target systems instructing them to send traffic via specific (hostile) machines.

Threat 9: Communications manipulation: Active interception, Insertion of false messages, Deliberate delivery out of sequence, Deliberate delay of delivery, Deliberate misrouting. If an attacker can force a message to be sent via a hostile host, the attacker may be in a position to intercept, alter and the forward the message.

Threat 10: Repudiation: This threat addresses cases of people denying that they sent a message (repudiation of origin), or that they received a message (repudiation of receipt).

Threat 11: Communications failure: Unavailability of Service Provider, Failure of data link, Non – delivery of message, Accidental delivery out of sequence, Accidental delay in delivery, Accidental denial of service. The Internet does not provide a service level agreement. There are no guarantees on how long it will take for a message to get to a recipient, or even that it will get there, eventually.

Threat 12: Embedding of malicious code: Includes email viruses and hostile mobile code (for example hostile Active X applets). Once on a network, they can quickly infect many machines causing significant disruption. Java and Active X raise a range of new security concerns. Users are now running code written by people from outside of the organisation, sometimes from unknown sources. This code has often not been tested by the organisation. There are concerns that hostile code written using these types of techniques could inflict damage on systems and networks.

Threat 13: Accidental misrouting: The threat of accidental misrouting covers the possibility that information might be delivered to an incorrect address when it is being sent over a network.

Threat 14: Technical failure of host: This threat covers failures of the CPU or other hardware items.
Threat 15: Technical failure of storage facility: This threat covers disk crashes and disk failures.

Threat 16: Technical failure of Print facility: This questionnaire identifies the factors that increase the threat for a technical failure of the print facility.

Threat 17: Technical failure of network Distribution Component: This threat addresses cases of network distribution components, such as bridges and routers, failure.

Threat 18: Technical failure of Network Management or Operational Host: This questionnaire identifies the factors that increase the threat of technical failure of a network management or operation host.

Threat 19: Technical Failure of Network Interface: Here, the factors that increase the threat of failure of the network interface are identified.

Threat 20: Technical failure of Network service: Here, the factors that increase the threat of failure of the network service are identified.

Threat 21: Power failure: This threat covers the possibility that the power supply to the building may fail. The types of power failure covered include: spikes, surges, brown outs, black outs.

Threat 22: Air conditioning failure: This threat covers the possibility that operation may have to be suspended because temperatures in the location fall outside of acceptable parameters.
Risk Management Categorisation

Description
Your Company Name has guidelines for all employees regarding risk management, categorisation and scoring.

Purpose & Scope
The purpose of this policy is to explain the general procedures relating to risk management, categorisation and scoring.

The following guidelines are to be adhered to by all employers, supervisors and employees.

Policy & Procedure
Risk Categorisation
For each risk, Your Company Name will identify a risk category. The categorisation of a risk identifies the type of risk and how it relates to the business. Some assets may have multiple risk categories associated, and therefore these need to be documented as well.

The below table provides an example of common risk categories used. Additional categories may be added during the Risk Assessment to support effective and efficient information security risk reporting practices:

<table>
<thead>
<tr>
<th>Description</th>
<th>Relates to (examples):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset / Asset Integrity</td>
<td>Critical infrastructure and equipment, Severe weather events, Cave-in, Fall-of-Ground, etc.</td>
</tr>
<tr>
<td>Environment</td>
<td>Tailings, Noise, Air, Protected Species, Tenements, Approvals, Closure Planning, etc.</td>
</tr>
<tr>
<td>Community / License to Operate</td>
<td>Indigenous Communities, Heritage Sites, etc.</td>
</tr>
<tr>
<td>Finance</td>
<td>Cashflow, Foreign Exchange, Tax, Reporting, etc.</td>
</tr>
<tr>
<td>Geoscience</td>
<td>Reserves, Ore Grade, etc.</td>
</tr>
<tr>
<td>Legal / Governance / External Affairs</td>
<td>Legal Compliance, Fraud, Reputation, etc.</td>
</tr>
<tr>
<td>Health and Safety</td>
<td>Carcinogens, Working at Heights, Drugs &amp; Alcohol, etc.</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Cyber Security, Data Integrity, Sensitive Information, Infrastructure, Availability, etc.</td>
</tr>
<tr>
<td>Joint Ventures</td>
<td>Joint Venture Agreements, JV Culture, etc.</td>
</tr>
<tr>
<td>Major Capital Projects</td>
<td>EPCM, 3rd Party Risks, Benefits Realisation, etc.</td>
</tr>
<tr>
<td>Marketing / Products</td>
<td>Price Protocols / Commodity Prices, Quality / Blending, Logistics, etc.</td>
</tr>
</tbody>
</table>
Consequences and Likelihood
In alignment with the Risk Management Framework, once the risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.

After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk, i.e. the probability that a threat will exploit the vulnerability of the respective asset.

By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk is calculated automatically by adding up the two values.

Existing security controls are to be entered in the last column of the Risk Assessment Table.

The tables below are examples of a Risk Management Framework: Risk and Control Assessment Criteria, Risk Likelihood Criteria, Risk Score.

Change and modify the details accordingly to your business, industry and company policies.

### Risk and Control Assessment Criteria

#### Effect / Consequence

<table>
<thead>
<tr>
<th>Loss Type</th>
<th>1 Insignificant</th>
<th>2 Minor</th>
<th>3 Moderate</th>
<th>4 Major</th>
<th>5 Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P) Harm to People</td>
<td>Slight injury or health effects – report only or first aid injury.</td>
<td>Minor injury or health effects – medical treatment injury or restricted work injury.</td>
<td>Serious bodily injury or health effects – lost time injury.</td>
<td>Single fatality</td>
<td>Multiple fatalities</td>
</tr>
</tbody>
</table>
| (E) Environmental Impact  | Environmen
tal nuisance – trivial or negligible, short term impact to area of low significance, minimal or no physical remediation required | Minor environmental harm – short term impact to area of limited local significance, limited physical remediation | Serious environmental harm – impact to Environment, physical remediation, potential or actual community health impacts or pollution or contaminatio
n. | Major environmental harm – long term reversible impact, health statistics in community may alter as a result of this incident or | Extreme environmental harm – irreversible impacts on environment al values of extreme & widespread areas, or those of national conservation significance, |

[Date]
<table>
<thead>
<tr>
<th>Asset Damage and Other Consequential Losses</th>
<th>Cost &lt; $1,000</th>
<th>Non-Compliance, potential warning notice, other notices (infringement / prosecution) unlikely.</th>
<th>Infringement Notice but Prosecution unlikely. Costs 50k - 250k</th>
<th>pollution or contamination Prosecution Costs &gt;250k - 1m</th>
<th>community fatalities or pollution or contamination Prosecution, License revoked Costs &gt; 1m</th>
</tr>
</thead>
<tbody>
<tr>
<td>(O) Slight damage &lt; 1m or &lt; 1-day disruption to operation</td>
<td>Local damage 1 - 5m or &lt; 1-week disruption to operation</td>
<td>Major damage $ 5 – 20m or &lt; 1-month disruption to operation</td>
<td>National impact – National public concern Temporary withdrawal of license to operate – significant brand damage</td>
<td>International impact - International public attention Loss of shareholder confidence – irreparable brand damage</td>
<td></td>
</tr>
<tr>
<td>(R) Impact on Reputation</td>
<td>Slight impact – Public awareness may exist but no public concern Isolated compliance failure – no brand damage</td>
<td>Limited impact – Some local public concern Intervention of regulating authority – minimal brand damage</td>
<td>Considerable impact - Regional public concern Major compliance failure involving fines – medium brand damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>slight impact – Public awareness may exist but no public concern Isolated compliance failure – no brand damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Likelihood Criteria &amp; Risk Score</td>
<td>Insignificant</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Almost Certain: Likely the unwanted event could occur several times per year in our jurisdiction</td>
<td>11</td>
<td>16</td>
<td>20</td>
<td>23</td>
<td>25</td>
</tr>
<tr>
<td>Likely: Likely the unwanted event could happen annually in our jurisdiction</td>
<td>7</td>
<td>12</td>
<td>17</td>
<td>21</td>
<td>24</td>
</tr>
<tr>
<td>Possible: The unwanted event could happen within XX years of our jurisdiction</td>
<td>4</td>
<td>8</td>
<td>13</td>
<td>18</td>
<td>22</td>
</tr>
<tr>
<td>Unlikely: The unwanted event could happen within</td>
<td>2</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>19</td>
</tr>
</tbody>
</table>
Rare: The unwanted event has never been known to occur or is highly unlikely that it could ever occur in our jurisdiction

| XX years of our jurisdiction | 1 | 3 | 6 | 10 | 15 |

Risk Acceptance Criteria
The total risk score for each asset threat and vulnerability is defined and calculated as per the Risk Management Framework:

- Values 1, 2, 3, 4 & 5 are LOW risks
- Values 6, 7, 8, 9, 10, 11, 12 are Medium risks
- Values 13, 14, 15, 16, 17, 18, 19 & 20 are HIGH risks
- Values 21, 22, 23, 24 & 25 are EXTREME risks

All risks need to be managed accordingly to business policies, and Unacceptable risks MUST be treated.