This is an accompanying appendix to the [Cybersecurity Toolkit for IT teams](https://www.csa.gov.sg/it-team-toolkit) developed by the Cyber Security Agency of Singapore (CSA). Within this appendix, you will find templates which your enterprise can adapt and use. Selected templates are also relevant for enterprises seeking certification for the [Cyber Essentials](https://www.csa.gov.sg/cyber-essentials) mark.

[Appendix 1 — Template for Cybersecurity Work Plan](#_Appendix_1_—)

[Appendix 2 — Template for Cybersecurity Risk Assessment](#_Appendix_2_—)

[Appendix 3 — Template for Cybersecurity Risk Management](#_Appendix_3_—)

**References for Cyber Essentials certification: “ASSET 🡪 Hardware and Software”**

[Appendix 4 — Template for Asset Inventory (Hardware)](#_Appendix_4_—)

[Appendix 5 — Template for Asset Inventory (Software)](#_Appendix_5_—)

[Appendix 6 — Template for Asset Management](#_Appendix_6_—)

**References for Cyber Essentials certification: “ASSET 🡪 Data”**

[Appendix 7 — Template for Asset Inventory (Data)](#_Appendix_7_—)

[Appendix 8 — Template for Data Management](#_Appendix_8_—)

[Appendix 9 — Template for Data Classification](#_Appendix_9_—)

**References for Cyber Essentials certification: “SECURE/PROTECT 🡪 Access Control”**

[Appendix 10 — Template for Account Inventory](#_Appendix_10_—)

[Appendix 11 — Template for Access Control](#_Appendix_11_—)

[Appendix 12 — Template for Passphrase](#_Appendix_12_—)

[Appendix 13 — Guidance on Strong Passphrases](#_Appendix_13_—)

[Appendix 14 — Template for Non-Disclosure Agreement](#_Appendix_14_—)

**References for Cyber Essentials certification: “SECURE/PROTECT 🡪 Secure Configuration”**

[Appendix 15 — Template for Configuration Management](#_Appendix_15_—)

[Appendix 16 — Template for Software Patch Management](#_Appendix_16_—)

**References for Cyber Essentials certification: “BACKUP 🡪 Back up Essential Data”**

[Appendix 17 — Template for Data Backup](#_Appendix_17_—)

**References for Cyber Essentials certification: “RESPOND 🡪 Incident Response”**

[Appendix 18 — Template for Incident Response Plan (including data breach)](#_Appendix_18—_Template)

[Appendix 19 — Template for Change Management](#_Appendix_19_—)

[Appendix 20 — Template for IT Acceptable Use Policy](#_Appendix_20_—)

[Appendix 21 — Template for Service Level Agreement (SLA)](#_Appendix_21_—)

[Appendix 22 — Template for Key Risk Indicator (KRI)](#_Appendix_22_—)

[Appendix 23 — Template for Business Impact Analysis (BIA)](#_Appendix_23_—)

[Appendix 24 — Template for Business Continuity Plan (BCP)](#_Appendix_24_—)

[Appendix 25 — Template for Disaster Recovery Plan (DRP)](#_Appendix_25_—)

[Appendix 26 — Template for Crisis Management Plan (CMP)](#_Appendix_26_—)

## Appendix 1 — Template for Cybersecurity Work Plan

|  |  |  |  |
| --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | |
| **Action Items** | **Roles and Responsibilities** | **Budget** | **Target Date of Completion** |
| List of actionable items to address the security controls and processes that need to be put in place | Roles and responsibilities of the owner/team/department carrying out the action item | Budget to be allocated for carrying out the action item | The date by which the action item is expected to be completed |
| Cultivating Cybersecurity Leadership | | | |
| … |  |  |  |
| Educating Employees on Cybersecurity | | | |
| e.g. Conducting training programmes to ensure employees are sufficiently aware of and educated on cybersecurity | e.g. **HR —** to provide an employee list and assign training to them, **IT —** Identify training materials/topics/engage vendors, **Compliance —** to ensure employees attend the training | e.g. $5,000/year | e.g. 11/1/2022 and thereafter, on an annual basis |
| … |  |  |  |
| Protecting Business-Critical Information Assets | | | |
| … |  |  |  |
| Securing the Access and Environment | | | |
| … |  |  |  |
| Ensuring the Business is Cyber Resilient | | | |
| … |  |  |  |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | |

## Appendix 2 — Template for Cybersecurity Risk Assessment

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | | | | | | | | |
| **Risk Type** | **Risk Description** | **Likelihood (L)**  **(1 - 5)** | **Impact (I)**  **(1 - 5)** | **Overall Risk Value  (L x I)** | **Risk Priority**  **(H/M/L)** | **Risk Response Strategy** | **Risk Treatment Activity** | **Assigned To** | **Due Date** | **Status** |
| i.e. Technical risk, operational risk, etc. | A detailed description of the risk, including the potential impact(s) | Rate 1-5 depending on how likely the risk is to occur, based on the organisation's environment | Rate 1-5 depending on the consequences of the risk on the organisation | Using the risk likelihood (L) and impact (I) to derive the overall risk value | Prioritise the risk based on the overall risk value to be High, Medium, or Low | To accept, mitigate, avoid or transfer | Activities carried out/ to be carried out in treating the risk | Specify the ownership or the team/department responsible for treating the risk | The date by which the risk should be treated | Whether the risk treatment activity has started, is in progress, or has been completed |
| e.g. Data breach | e.g. Use of unauthorised portable storage devices (e.g. USB drives) to transfer confidential and/or sensitive data | e.g.  1 — Rare  2 — Unlikely  3 — Possible  4 — Likely  5 — Highly Likely | e.g.  1 — Minor  2 — Moderate  3 — Significant  4 — Serious  5 — Major | e.g. 3x2=6 | e.g. Low= 1-4, Medium= 5-9, Medium High= 5-12, High= 12-16, Critical= 17-25 | e.g. Mitigate/ Accept/ Transfer/ Avoid | e.g. Sent email reminders to only attach authorised devices to the endpoints | e.g. IT Team | e.g. 1/1/2022 | e.g. In Progress |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | | | | | | | | |

## Appendix 3 — Template for Cybersecurity Risk Management

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  What is cybersecurity risk management and what are the steps to perform risk management.  **<Purpose>**  The purpose is to provide a common methodology and approach to ensure that risks in the organisation are identified, assessed, analysed, evaluated, treated, and monitored to a satisfactory level.  **<Scope>**  It includes the systems and information assets in the organisation that this policy is applicable to.  **<Roles and Responsibilities>**  The roles and responsibilities of the personnel involved in risk management — from assessment to maintaining and monitoring, and eventually treating the risks to ensure that they have been remediated.  **<Risk Identification>**  This section is the first step of risk management to identify the potential risks in the environment, and any uncertainties or things that could go wrong. The risks could be categorised according to the nature of the risks, e.g. strategic, financial, operational risks, etc. and be documented.  **<Risk Analysis>**  The next part of risk management is to analyse the risks by assessing the likelihood and measuring the impact, e.g. using a 5-scale rating i.e. 1—very low, 2—low, 3—medium, 4—high, and 5—very high. Refer to the example of a Risk Heat Map under <Risk Evaluation> for the graphical representation of the measurement scale for the likelihood and impact.  **<Risk Evaluation>**  Based on the result of risk analysis and any other considerations from the stakeholders, the risks can be ranked according to priority. Refer to the below example of a Risk Heat Map for the graphical representation of risk evaluation based on the likelihood and impact.   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Likelihood** | 5 — Very Likely | 5 (e.g. 5-9 to be under medium risk level) | 10 (e.g. 10-12 to be under medium high-risk level) | 15 (e.g. 13-16 to be under high risk level) | 20 (e.g. 17-25 to be under critical risk level) | 25 | | 4 — Likely | 4 | 8 | 12 | 16 | 20 | | 3 — Possible | 3 | 6 | 9 | 12 | 15 | | 2 — Unlikely | 2 | 4 | 6 | 8 | 10 | | 1 — Very Unlikely | 1 (e.g. 1-4 to be under low risk level) | 2 | 3 | 4 | 5 | |  | 1 — Minor Impact | 2 — Moderate Impact | 3 — Significant Impact | 4 — Serious Impact | 5 — Major Impact | | **Impact** | | | | | | |   **<Risk Treatment>**  This section is to consider the options available and to apply the various controls and measures to ensure the risks are assigned to be treated by the risk owner through any of the risk response strategies, i.e., risk avoidance, acceptance, mitigation, and transfer.  **Risk Avoidance —** This includes avoiding the risks through adopting an alternative strategy or approach.  **Risk Acceptance —** This includes accepting the risk or sharing it through collaboration with other companies.  **Risk Mitigation —** This includes steps to manage and reduce the risk to an acceptable level.  **Risk Transfer —** This includes the reduction of risk by shifting it to a third party e.g. an insurance company.  **<Risk Monitoring>**  The final step of risk management is to monitor the progress of the risk treatment and to ensure that it does not exceed the level of risks acceptable to the organisation.  **<Risk Review and Reporting>**  Risk assessment should be carried out on a regular basis to ensure any key or new findings have been identified and documented in the risk register and are reported to the senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## 

## Appendix 4 — Template for Asset Inventory (Hardware)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | | | | | | | |
| **Hardware Name/ Model** | **Asset tag[[1]](#footnote-1)/**  **serial number** | **Asset Type** | **Asset Location** | **Network Address** | **Asset Owner** | **Asset Classification** | **Department** | **Approval/ Authorised Date** | **EOS Date** |
| Name and model of the asset | Unique identifier for the asset | Grouping of assets based on its characteristics and function | Location where the asset is situated in the organisation | The IP or MAC address of the asset | Personnel responsible for overseeing and maintaining the asset | Grouping of assets based on sensitivity level and impact of compromise | The department using this asset | Date when the asset has been approved and authorised for use | Date when the asset will no longer receive support from the product vendor |
| e.g. ASA5505-BUN-K9 Cisco ASA 5505 Firewall | e.g. FW2000001 | e.g. Firewall | e.g. Data Centre 1, Serangoon North Ave 5 | e.g. 00:17:C5:E1:T7:4Y | e.g. IT Infra Manager | e.g. Critical | e.g. Network | e.g. 1/1/2022 | e.g. 10/1/2030 |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | | | | | | | |

## Appendix 5 — Template for Asset Inventory (Software)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | | | | |
| **Software Name** | **Software Publisher** | **Software Version** | **Business Purpose** | **Asset Classification** | **Approval/ Authorised Date** | **EOS date** |
| Name of the asset | The publishing company of the asset | Version of the asset | The purpose and use of the asset | Grouping of assets based on sensitivity level and impact of compromise | Date when the asset has been approved and authorised for use | Date when the asset will no longer receive support from the product vendor |
| e.g. Oracle Fusion Cloud ERP | e.g. Oracle | e.g. Version 1.3 | e.g. Financial accounting | e.g. Internal | e.g. 10/10/2022 | 1/1/2030 |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | | | | |

## Appendix 6 — Template for Asset Management

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.* *Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Cybersecurity asset management is the process of identifying, continuously, the hardware and software in the organisation to identify the potential security risks. It is needed to ensure that the assets are (i) authorised to access the enterprise environment, and (ii) secured properly to reduce the total cost of risks related to asset management.  **<Purpose>**  The purpose is to protect organisation assets by preventing unauthorised disclosure, modification, removal, or destruction of information assets that may lead to interruptions in business activities.  **<Scope>**  This policy or guideline applies to all parties operating within the organisation environment, and all the assets owned by the organisation.  **<Roles and Responsibilities>**  The roles and responsibilities of employees who are involved in asset management include:   1. Asset manager: [Designation] 2. End users   **<Asset Management Lifecycle>**  The asset management lifecycle comprises the infrastructure and processes necessary for the effective management, control, and protection of the assets within the organisation, throughout its lifecycle.   1. Planning:    * Establish the requirement of an asset    * Identify the need for the asset 2. Get approval/authorisation from [designation] for the procurement of the asset. 3. Procurement:    * Ensure assets procured are as per the required specification.    * Check status of assets and update the relevant inventory. 4. Onboarding:    * Ensure checks are being done before onboarding assets into the organisation’s environment.    * Seek approval from [designation] to onboard new assets.    * Update inventory once assets are onboarded. 5. Monitoring and Maintenance:    * Monitor assets periodically and check for any performance issues that could unexpectedly develop, e.g. monitor End-of-Life (EOL) and End-of -Support (EOS).    * Conduct yearly asset audit to assess assets.    * Perform periodic maintenance to ensure that all assets are maintained. 6. Disposal:    * Assets shall be disposed of after EOL/EOS.    * If the organisation intends to continue using an EOS asset, assess the risk and obtain approval from [designation]. Actively monitor the EOS asset until it is replaced. 7. Assets containing information valued as critical and vital shall be disposed of securely and safely. All confidential information shall be deleted prior to disposal, and the asset disposed of securely and completely.   **<Review Schedule>**  The policy or guideline should be reviewed and signed off [bi-annually] with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 7 — Template for Asset Inventory (Data)

|  |  |  |  |
| --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | |
| **Description** | **Asset Classification** | **Asset Location** | **Retention Period** |
| Description of the data asset | Grouping of assets based on sensitivity level and impact of compromise | Location where the asset resides at in the organisation | The duration the asset should be kept and retained by the organisation |
| e.g. Customer’s phone number | e.g. Confidential | e.g. Database | e.g. Retained for 14 days before carrying out destruction |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | |

## Appendix 8 — Template for Data Management

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Data is the enterprise’s most valuable business asset. Identifying the critical data in the enterprise is the key foundational step to classify, monitor, and protect it to ensure that only authorised personnel can access it.  **<Purpose>**  The purpose is to classify data based on its sensitivity, value, and impact as the result of a compromise to the organisation, so that sufficient measures can be carried out to protect them.  **<Scope>**  This policy or guideline applies to all parties operating within the organisation environment, and all the business-critical data assets owned by the organisation.  **<Roles and Responsibilities>**  The roles and responsibilities of the employees involved in carrying out and maintaining the data classification:   1. Data owner: [Designation] 2. Data custodian: [Designation]   **<Data Classification>**  The procedures to carry out data classification, based on the sensitivity level and overall business impact to the organisation.  **<Data Protection and Handling>**  The following data protection and handling measures that are in place include:   * Protection of business-critical data through [password protection | encryption of data] * Secure deletion of data from media before secure disposal * Shredding of paper-based data (hard copy) before secure disposal   **<Data Loss Prevention>**  The following data loss prevention measures and controls that are in place to restrict the leakage and loss of confidential and/or sensitive data include:   * Disabling USB drives and enforcing policies on the use of external disks * Imposing guidelines that should be adhered to by all the employees, e.g. Not sending any company information to private email address   **<Reporting of data breach and compromise>**  Suspected data breaches and compromise within the organisation should be reported to: [designation]  **<Review Schedule>**  The policy or guideline should be reviewed and signed off [bi-annually] with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## 

## Appendix 9 — Template for Data Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | | |
| **Data classes:** | **Class 1 — Restricted** | **Class 2 — Confidential** | **Class 3 — Internal** | **Class 4 — Public** |
| **Definition** | Highly sensitive business data that are protected by law, used to identify a person, and if compromised, would put the organisation at significant financial risk | Sensitive data that is only available for use by authorised employees and if compromised, would affect the operations of the organisation negatively | Data that is only available to all employees and not meant for public disclosure | Data that falls within the public domain and is freely available to everyone within and beyond the organisation |
| **Impact of loss** | Severe business disruption, loss of reputation, public backlash, and legal implications | Moderate loss of reputation, public backlash, and public gaining knowledge of the organisation’s internal processes | Low to medium business disruption | Little to no business impact |
| **Examples** | Employee’s record, Personal Identifiable Information, financial statements, medical records, contracts | Business plans and business strategy documents, network diagrams, application source codes | Company announcements, newsletters, organisation charts | Website information, press releases, marketing materials, contact information |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | | |

## Appendix 10 — Template for Account Inventory

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | | | |
| **Name** | **Username/email** | **Department** | **Role/Account Type** | **Date of access created** | **Last logon date** |
| Name of the employee/ account | Unique ID/username for the account or email address | Department of the employee | Account role/ type e.g. Administrator, service account | Date when the access was created | Date when the account was last logged on |
| e.g. Tan Ah Hock | e.g. Hock12 | e.g. Logistics | e.g. Operator account | e.g. 12/10/2022 | e.g. 20/10/2022 |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | | | |

## Appendix 11 — Template for Access Control

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.* *Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Active user accounts and physical access are the source of entry to the hardware and software in the enterprise environment. Ensuring that only authorised users are given the access rights they need to perform their work helps reduce the risk of information being stolen, or hardware and software being compromised.  **<Purpose>**  The purpose is to ensure that access controls are implemented and to protect the sources of entry to the hardware and software in the enterprise environment.  **<Scope>**  This policy or guideline applies to all employees and third parties, including suppliers who have access to the organisation’s systems, data, and resources.  **<Roles and Responsibilities>**  The roles and responsibilities of employees involved in carrying out and maintaining access controls:   1. Requestor: End users 2. Approver: [Designation] 3. Administrator: [Designation]   **<Principle of least privilege>**  Access control is assigned on the basis of business needs and ‘Least Privilege’. Users must only be provided with the absolute minimum access rights and permissions to systems, data, and resources that they need to fulfil their job roles.  **<User access account management>**  User account management procedures must be implemented for the following:   1. Account creation, modification, and deletion 2. Account monitoring    * Ensure there are no shared, duplicate, obsolete, or invalid accounts    * Ensure dormant or accounts that have been inactive for a prolonged period [30 days] are removed or disabled    * Removal of accounts with access rights that are no longer required or have exceeded the requested date 3. Use of administrator accounts – Limited to performing administrator functions, with approval from senior management [designation] 4. Account locking or disabling after [10] failed login attempts 5. Logging of    * All creation, modification, and deletion of system and user access    * Login attempts 6. Regular reviews of system and user access   **<Process for granting and revoking of access>**  The process to request to grant and revoke access includes the following:   1. Requestor ensures the need for access to be granted/revoked and sends in a request, providing    * Name and department of employee    * System to access    * Role/account type requested    * Duration for access 2. Approver to review the request 3. If the request is approved, Administrator to grant/revoke access accordingly 4. Administrator to notify the requestor on the access changes for confirmation   **<Process to request for administrative access to system>**  The process to request to grant and revoke access includes the following:   1. Requestor ensures that administrative access is required and sends in a request 2. Approver to review the request 3. If the request is approved, Administrator to create the account and notify the requestor 4. Administrator to notify the requestor on the access changes for confirmation   **<Process for granting and revoking of physical access>**  The process to request to grant and revoke physical access to assets includes the following:   1. Requestor ensures that physical access has to be granted/revoked and sends in a request 2. Approver to review the request 3. If the request is approved, Administrator to grant/revoke access accordingly 4. Administrator to notify the requestor on access changes for confirmation 5. Administrator to notify the physical access control team   **<Passphrase management>**  Refer to Appendix 12 – Template for Passphrase  **<Review Schedule>**  The policy should be reviewed and signed off [quarterly] with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 12 — Template for Passphrase

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  A strong passphrase provides the first line of defence against unauthorised access to the organisation’s system, network, or data. A stronger passphrase provides better protection from hackers and malicious software.  **<Purpose>**  The purpose is to establish standards and guiding principles for setting strong passphrases.  **<Scope>**  This policy or guideline applies to all the accounts (e.g. service or privileged account) of systems and networks in the organisation.  **<General Guidelines>**  All systems-level passphrases (e.g. root, administrator accounts) must be changed at least every [90] days.  All user-level passphrases (e.g. email, web) must be changed at least every [90] days, and the past [10] passphrases shall not be re-used.  **<Passphrase Requirement>**  All passphrases must conform to the prescribed guidelines. Refer to Appendix 12 – Guidance on Strong Passphrases.  **<Passphrase Protection>**  Passphrases must be protected from unauthorised disclosure, stored securely, and prevented from being transmitted in the open.  Passphrases should not be   * Revealed to anyone, or on questionnaires or forms * Written down and stored in an open area * Stored in an unprotected file on computer system   **<Passphrase Change>**   1. The passphrase needs to be changed and updated under these circumstances to ensure that access to user accounts is not being compromised. 2. Immediately after installation, all default system and vendor passwords must be changed. 3. In the event of any suspected compromise, the account passphrases shall be changed.   **<Review Schedule >**  The policy or guideline should be reviewed and signed off [annually] with the date and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 13 — Guidance on Strong Passphrases

|  |  |  |
| --- | --- | --- |
| **No.** | **Strong passphrase guiding principles** | **Explanation** |
| **1** | Passphrase is at least twelve characters long | Having a longer passphrase is typically more secure than a complex passphrase as they are harder to brute force. Based on industry best practices and guidelines for security standards on password policy, it is recommended for passphrases to be at least twelve characters long. |
| **2** | Passphrase is mixed with upper case, lower case, numbers, and/or special characters | Having a complex passphrase can help to further increase the strength of a passphrase by expanding the possible combination. The passphrase can consist of upper case and lower-case letters, numbers and/or special characters in any order. |
| **3** | Passphrase is made up of five random words that are easy to remember | A passphrase consisting of around five random words serves the same function to increase the strength of the passphrase by making it long and unpredictable, yet easy to remember. |
| **4** | Passphrase is unpredictable | Using a default or predictable passphrase makes it easier for attackers to crack it by brute force. For example, one of the most commonly used passwords, ‘111111’, has been used over 13 million times in 2021. |
| **5** | Passphrase is unique for different accounts | Using a passphrase that is unique across every account would mean that in the event of a passphrase compromise, the other accounts belonging to the same user would not be exposed to the risks, as compared to if they were all using the same passphrase. The trade-off is that the user would need to remember which passphrase was used for each account. |
| **7** | Passphrase need not be changed frequently unless it has been, or is suspected of being, compromised | Excessive changing of passphrases can bring more harm than good, as users would constantly be forced to come up with new passphrases. They would also be more likely to come up with a predictable passphrase based on their old passphrase, e.g. increase the number sequentially from “password1” to “password2”. The trade-off is that an employee’s passphrase that has been compromised unknowingly can be used by cyber attackers for a prolonged period of time without anyone noticing. |

## Appendix 14 — Template for Non-Disclosure Agreement

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Overview>**  To protect and prevent the use and disclosure of the business’s confidential information by a third party  **<Purpose>**  The purpose is to lay out the obligations and exceptions to obligations of the recipient party  **<Scope>**   1. Parties involved: It applies to every party who signed the Non-disclosure Agreement for all confidential information of the business 2. Clauses of agreement: Rules and principles for the confidentiality of the information to be exchanged   **<Timeframe>**  The timeframe for which the agreement is effective  **<Sign Off>**  The sign offs from the recipient party |

## Appendix 15 — Template for Configuration Management

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Configuration management is the process of managing the configurable components or resources of a system or environment on which a software application runs to ensure these resources and components maintain a consistent, or baseline, state. It is important to ensure the organisation has visibility over the secure configuration of its assets and maintains effective control of its IT systems.  **<Purpose>**  The purpose is to ensure the assets in the organisation are being configured securely against a baseline that is compliant with the IT security policies, standards, and procedures.  **<Scope>**  It includes both hardware (e.g. network devices, end points, mobile devices) and software (e.g. anti-virus) that are configurable and that pose a threat to the organisation’s production environment if compromised.  **<Roles and Responsibilities>**  The roles and responsibilities of employees involved in configuration management:   1. Configuration management sponsor: [Designation] 2. Configuration manager: [Designation]   **<Security Baseline Configuration>**   1. The assets should be configured and secured based on widely accepted and well-established security standards and benchmarks.  * Avoid or update weak or default configurations.  1. Replace or upgrade insecure configurations and weak protocols. 2. Reviews should be regularly carried out to update the configuration. 3. Retain the previous configuration as a form of contingency. The configurations and security standards referenced should also be tracked and documented as part of an asset configuration list. 4. Disable or remove features, services, or applications that are not in use.  * Disable automatic connection to open networks and the auto-run feature of non-essential programs.   **<Configuration Change Control>**  Changes in configuration to assets shall be reviewed and approved by authorised personnel with the relevant change documents, risk assessment, impact analysis and contingency plan which have been tested and verified before deployment to the production environment.  **<Logging>**  Logging should be enabled by default and saved to a central repository that is kept secure against unauthorised access to assist in carrying out diagnosis, troubleshooting or reconciliation of events.  **<Conformity to configuration standards>**  Put in place a process to ensure that the systems in scope conform to the security baseline configuration. Any deviation or non-conformance should be reviewed, monitored, approved, and reported to the senior management with sufficient mitigating controls in place. Employees who violate this policy may also be subjected to disciplinary actions.  **<Review Schedule>**  The policy or guideline should be reviewed and signed off [annually] with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 16 — Template for Software Patch Management

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Software patch management is the process of distributing and applying updates to software. These patches are necessary to update, fix, or enhance the software, including fixing security vulnerabilities, as well as protecting software and operating systems from exploitation.  **<Purpose>**  The purpose is to secure the organisation by ensuring an appropriate patch management policy is in place.  **<Scope>**  This policy or guideline applies to all hardware and software used in the organisation’s systems.  **<Roles and Responsibilities>**  The roles and responsibilities of the employees involved in patch management:   1. Patch manager: [Designation or role in organisation] 2. End users   **<Patch Management Process>**  The patch management process includes the following:   1. Visiting official sources for vulnerabilities, patches, and updates. 2. Maintaining an up-to-date inventory of hardware and software assets to allow tracking of the latest patches. 3. Testing of patches. This would be done in a test environment before roll out to ensure that the production environment is not affected after the patch. For smaller organisations, it would be recommended to test the patches on the least critical servers that could be easily recovered in case of a system failure. 4. Developing and implementing a patch schedule which includes automated and manual patching to ensure all patches are applied regularly and timely. 5. Monitoring of patches deployed to ensure that that there is no repercussion and the system or device patched is still functioning as it was before.   **<Review Schedule>**  The frequency of when the policy should be reviewed and signed off with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 17 — Template for Data Backup

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Data backups are critical in enabling quick recovery from cyber security incidents such as ransomware or malware, but also physical incidents such as system failure, theft, or natural disasters.  **<Purpose>**  The purpose is to create a backup plan that allows the business to continue its operation after a system failure or incident.  **<Scope>**  The policy or guideline includes all types of media format (e.g. hard disk, magnetic tape), data, and personnel.  **<Roles and Responsibilities>**  The roles and responsibilities of the employees involved in carrying out, maintaining, and restoring a data backup:   1. Backup manager: [Designation] 2. End users   **<Types of Backups>**  **Full backup —** The complete data is backed up and stored, and as such it requires the most space and time to complete — but is restored in the shortest time. Used for completeness of data.  **Differential backup —** Performs backup faster and requires less space than a full backup, but performs backup slower than an incremental backup, and slower restoration than a full backup. Used when downtime and cost need to be minimised.  **Incremental backup —** Perform the fastest backup with the least amount of space required, but with the slowest restoration time compared to a full and differential backup. Used when backup speed is of top priority and where site-to-site backup is limited.  **<Backup Schedule>**  [Type of data, e.g. more critical data]   * Frequency: [Daily] * Type of backup: [Automated]   [Type of data, e.g. less critical data]   * Frequency: [Monthly] * Type of backup: [Manual]   **<Backup Storage, Retention and Destruction>**   * Backup data and logs should be   + Stored securely, and protected from unauthorised access through physical and logical security controls   + Retained for at least [duration] * Deleted securely to purge off the data completely and with secure destruction carried out when no longer needed * Backup of critical-business data should be stored offsite   **<Backup Recovery Test>**   * Data recovery testing should be performed. * The frequency, testing procedures, and the testing outcomes should be documented and reported to senior management. * Steps to be carried out by the personnel in data backup and restoration should be clearly documented for testing with improvement points that can used to update the data backup policy.   **<Review Schedule>**  The policy or guideline should be reviewed and signed off [annually] with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 18— Template for Incident Response (including data breach)

|  |  |
| --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | |
| 1. **Preparation**  Preparation for an incident response is not just about preparing to handle an incident when it happens. It also entails the prevention of incidents by ensuring that systems, networks, and applications are sufficiently secure. | |
| Preparing to handle incidents | Identify key contact information:  ◻ Designate an incident response handler within your organisation  ◻ Designate a data breach management team within your organisation. The team should comprise specific individual(s) with expertise  in handling data breaches, the data protection officer (“DPO”), and a senior management representative  ◻ Appoint a third-party incident response provider  ◻ Contacts for product/service vendor(s)  ◻ Regulatory bodies  ◻ Law enforcement agencies  ◻ SingCERT  ◻ Clients  ◻ Personal Data Protection Commission (PDPC) (if an organisation collects, uses and/or discloses individuals’ personal data)  ◻ Others: \_\_\_\_\_\_\_\_ |
| Recognising possible attack vectors | Organisations should generally be prepared to handle any incidents, including data breaches. They can first identify and understand the types of attacks that could affect the organisation (which may also result in a data breach), then develop action plans to deal with each type of attack.  Common attack vectors or entry points that threat actors may use are :  ◻ Malware  ◻ Phishing  ◻ Distributed denial of service  ◻ Ransomware  ◻ Data breach  ◻ Data corruption  ◻ Poorly designed web applications  ◻ Misconfigured systems  ◻ Internet downloads  ◻ Poor cyber hygiene practices (e.g. use of weak or default passwords, use of outdated software, etc.)  ◻ Human lapses  ◻ Authorised third parties  ◻ Others: \_\_\_\_\_\_\_\_  Possible activities that may result in a data breach include but are not limited to:  ◻ Hacking, ransomware, distributed denial of service incidents or unauthorised access to databases containing personal data  ◻ Unauthorised modification or deletion of personal data  ◻ Theft of computer notebooks, data storage devices or paper records containing personal data  ◻ Scams (e.g., phishing attacks) that trick organisations into releasing personal data of individuals  ◻ Loss of computer notebooks, data storage devices, or paper records containing personal data  ◻ Sending personal data to a wrong email or physical address, or disclosing personal data to a wrong recipient  ◻ Unauthorised access or disclosure of personal data by employees  ◻ Improper disposal of personal data (e.g. hard disk, storage media or paper documents containing personal data sold or discarded before data is properly deleted)  ◻ Others: \_\_\_\_\_\_\_\_ |
| Reviewing possible sources of precursors and indicators | ◻ Security software (e.g. Intrusion Detection Systems [IDS], Security Information and Events Management System [SIEM], anti-virus software, third party monitoring services, etc.)  ◻ Logs (e.g. operating system logs, service and application logs, network device logs, netflow logs, etc.)  ◻ Publicly available information (e.g. SingCERT alerts, alerts from products/services vendors on vulnerabilities, etc.)  ◻ People from your organisation  ◻ Others: \_\_\_\_\_\_\_\_ |
| Develop, communicate, and exercise the plans | Develop relevant plans:  ◻ Prevention and detection plans  ◻ Containment, eradication, and recovery plans  ◻ Crisis management and communications plans  ◻ Business continuity plans  ◻ Data breach management plans  ◻ Others: \_\_\_\_\_\_\_\_  Action plans developed to respond to common incidents should be accessible, and any updates should be communicated to relevant parties (e.g. employees, vendors, etc.):  ◻ Communications with employees and key stakeholders  ◻ User awareness and training  ◻ Regular reviews and updates of plans (e.g. when systems are onboarded, to new hires, or at regular scheduled intervals)  ◻ Walk-through/exercise the plans  ◻ Others: \_\_\_\_\_\_\_\_ |
| 2. **Detection and Analysis**  The detection and analysis of an incident is the first step to identifying an incident and understanding its impact and severity. | |
| Making an initial assessment and prioritising the next steps | ◻ Correlate events against the baseline to determine if an incident has occurred  ◻ Check incidents against known threats precursors and indicators  ◻ Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch  ◻ Prioritise the incident handling activities, including whether to activate crisis management, and crisis communications plans  ◻ Others: \_\_\_\_\_\_\_\_  If a data breach has been discovered/is suspected to have occurred, the data breach management team will conduct an initial assessment to determine the severity of the data breach. The initial assessment should include the following considerations:  ◻ Cause of the data breach and whether the breach is still ongoing  ◻ Number of affected individuals  ◻ Type(s) of personal data involved  ◻ The affected systems, servers, databases, platforms, services, etc.  ◻ Whether help is required to contain the breach  ◻ The remediation action(s) that the organisation has taken or needs to take to reduce any harm to affected individuals resulting from the breach  ◻ Others: \_\_\_\_\_\_\_\_ |
| Gathering evidence | Evidence gathering may serve two purposes – incident resolution and legal proceedings. Some of the evidence that need to be documented include:  ◻ Summary of the incident  ◻ Incident indicators  ◻ System events  ◻ Actions taken during the incident  ◻ Logs of affected systems  ◻ Forensic copies of affected systems  ◻ Others: \_\_\_\_\_\_\_\_ |
| Knowing your stakeholders and/or fiduciary obligations | Notify relevant stakeholders and affected parties  ◻ Board of Directors  ◻ Regulators, law enforcement and other government agencies (SPF, CSA, SGX, PDPC etc.)  ◻ Clients  ◻ Media  ◻ Others: \_\_\_\_\_\_\_\_  An organisation should act swiftly as soon as it is aware of a data breach, whether suspected or confirmed.  ◻ Upon the discovery of a data breach (suspected or confirmed), staff are to report the breach to the Business Unit (BU) heads.  ◻ BU heads are to inform the Data Protection Officer (DPO) regarding the potential data breach.  ◻ DPO is to activate the data breach management team and update senior management on the potential data breach.  ◻ Others: \_\_\_\_\_\_\_\_ |
| 3. **Containment, Eradication & Recovery**  This is one of the most critical stages of incident response. The strategy for containment and recovery is based on the information and indicators of compromise gathered during the analysis phase. The threat needs to be thoroughly eradicated before normal operations can resume to minimise subsequent repeated disruptions. | |
| Developing a Containment Strategy | Containment strategies vary depending on the type of incident, and a strategy should be developed for different incident types to contain the incident/data breach and minimise damage. Some of the more common strategies are:  ◻ Isolate all or parts of the compromised network by disconnecting all affected systems  ◻ Re-route or filter network traffic  ◻ Prevent further unauthorised access to the system. Disable or reset the passwords of compromised user accounts  ◻ Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system  ◻ Firewall filtering  ◻ Close vulnerable ports and mail servers  ◻ Block further unauthorised access to the system  ◻ Stop the identified practices that led to the data breach  ◻ Establish whether the lost data can be recovered and implement further action to minimise any harm caused (e.g. remotely disabling a lost notebook containing a personal data of individuals, recalling an email that has been accidentally sent or forwarded etc.)  ◻ Others: \_\_\_\_\_\_\_\_ |
| Eradicating the threat | After containing the incident, eradication may be necessary to eliminate all traces of the incident. This may include:  ◻ Wiping out the malware  ◻ Disabling breached user accounts  ◻ Patching vulnerabilities that were exploited. This should be applied to all affected hosts within the organisation  ◻ Others: \_\_\_\_\_\_\_\_ |
| Assessing the data breach | If a data breach has occurred, upon the containment of the data breach, the data breach management team shall conduct an in-depth assessment of the data breach, the success of its containment action(s) taken, and the efficacy of any technological protection applied on the personal data involved in the data breach.  The data breach management team shall consider the following in the assessment of the data breach:  ◻ Context of the data breach  ◻ Ease of identifying individuals from the compromised data  ◻ Circumstances of the data breach  Crucially, the organisation will also have to determine if it is required to notify the PDPC and/or affected individuals of the breach as required by the PDPA. |
| Reporting data breaches to PDPC | In the case of a data breach, the DPO shall notify relevant stakeholders and affected parties from the time the data breach management team has determined that the data breach is notifiable under the PDPA.  ◻ Regulators, law enforcement and other government agencies, such as the PDPC, as soon as practicable, but in any case, no later than three (3) calendar days  ◻Affected individuals as soon as practicable, at the same time or after notifying the PDPC  ◻ Others:  **Note:** Organisations may refer to the PDPC’s Guide on Managing and Notifying Data Breaches under the PDPA for more information. |
| Taking steps towards recovery | This may entail:  ◻ Restoring systems from backups  ◻ Rebuilding systems from scratch  ◻ Changing passwords (both administrators and users)  ◻ Tightening network perimeter security  ◻ Confirming the integrity of business systems and controls  ◻ Others: \_\_\_\_\_\_\_\_ |
| Monitoring and maintaining vigilance | ◻ Continue to monitor the network for any anomalous activity or signs of intrusion  ◻ Depending on the incident, organisations may need to consider higher levels of system logging or network monitoring  ◻ Others: \_\_\_\_\_\_\_\_ |
| 4. **Post-Incident Review**  Organisations should proactively review their plans and response activities to identify and resolve deficiencies and strengthen their security posture. | |
| Conducting post-incident review | ◻ Identify and resolve deficiencies in systems and processes that led to the incident  ◻ Identify and resolve deficiencies in planning and execution of your incident response plan  ◻ Assess if additional security measures are needed to strengthen the security posture of your organisation  ◻ Communicate and build on lessons learnt  ◻ Others: \_\_\_\_\_\_\_\_  If a data breach has occurred, the data breach management team shall review and learn from the data breach to improve on their personal data handling practices. The review may involve the following:  ◻ A review including a root cause analysis of the data breach  ◻ A prevention plan to prevent similar data breaches in future  ◻ Audits to ensure prevention plan is implemented  ◻ A review of existing policies, procedures, and changes to reflect the lessons learnt from the review  ◻ Changes to employee section and training practices  ◻ A review of data Intermediaries involved in the data breach  ◻ Others: \_\_\_\_\_\_\_\_ |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | |

## Appendix 19 — Template for Change Management

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it. Text indicated in square brackets [] may vary from organisation to organisation.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  Change management refers to a structured process to review changes to the system or service. This process takes place prior to implementing the change on the organisation’s system or network, thus minimising impact of outrages on operations.  **<Purpose>**  The purpose is to ensure the implementation of change management and control strategies to mitigate risks.  **<Scope>**  This policy or guideline applies to all parties operating within the organisation environment. This also covers all the organisation systems, data, and resources.  **<Roles and Responsibilities>**  The roles and responsibilities related to change management:   1. Change Requestor: The person or department initiating the change. 2. Change Manager: The person responsible for the proper execution of the change management process. This would include changing the request status, leading the review board, coordinating changes, and reporting. 3. Change Review Board: Consists of a group of advisors, including different stakeholders, and is led by the Change Manager who reviews change requests, makes decisions and makes sure of a successful change implementation and follow-up.   **<Types of Changes>**   1. Emergency Change: A change that should be evaluated and implemented as soon as possible after the occurrence of a disruption. 2. Standard Change: A low-risk and low-impact change in which a specific procedure to follow is already pre-defined, documented, and is usually pre-approved, which makes the process shorter. 3. Major Change: A high-risk and high-impact change which could affect operations if not properly planned. This change requires detailed planning and management approvals. 4. Minor Change: A considerable low-risk and low-impact change which undergoes the whole change management process, including the Change Review Board and approvals.   **<Change Management Process>**  The change management process consists of various stages:   1. Request for Change (RFC): Submission of change request with detailed specification of the change. 2. Change Review: The change request will be reviewed by the Change Review Board based on the specifications and requirements. 3. Change assessment and planning:    * Risk assessment will be conducted on the agreed specification. Systems and processes affected by the proposed change will be assessed to identify any risks to the business.    * Implementation plan to detail all the stages required in order to successfully manage the change. This would include the test plan, roll back strategy, and timeline. 4. Change approval: Seek approval from the responsible parties in order to initiate the changes that have been planned. 5. Change implementation: Implementation of the change according to the implementation plan and the scheduled timeline. 6. Post implementation review: Post implementation, it is important to review and monitor the situation and identify any problems that could be prevented in the future, or improvements to be done.   **<Review Schedule>**  The policy or guideline should be reviewed and signed off [annually] with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 20 — Template for IT Acceptable Use Policy

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  The IT Acceptable Use Policy serves to govern and protect the IT resources and equipment in the organisation to minimise risks and damages as a result of improper or insecure usage.  **<Purpose>**  The purpose of this policy is to establish a framework consisting of the rules and guidelines to govern the organisation’s IT resources through proper and secure usage of the IT resources in the organisation.  **<Scope>**  This policy applies to all employees and suppliers who have access to the organisation’s IT resources. The scope of the IT resources includes hardware and software connected to and accessed through the organisation’s network, e.g. printers, emails, mobile devices, etc.  **<General>**  General guidelines and rules of the Dos and Don’ts, e.g. do not engage in unlawful activities, tamper with the IT resources, etc.  **<Hardware>**  Specific guidelines and rules of the Dos and Don’ts when using and handling any in-scope hardware systems, e.g.   * Do connect corporate devices to only trusted network connections when using them to access organisation data * Do not leave your corporate devices unattended and unlocked * Attach only approved USB devices to corporate devices   **<Software>**  Specific guidelines and rules of the Dos and Don’ts when using and handling any in-scope software and applications, e.g.   * Do not open email attachments or files downloaded from untrusted or unverified sources * Do check that the software is licensed and supported by updates   **<Reporting of violation and security events>**  The user’s responsibilities in reporting any violations of the policy, or suspected security events, and in taking the necessary corrective actions.  **<Review Schedule>**  The frequency of when the policy should be reviewed and signed off with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 21 — Template for Service Level Agreement (SLA)

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  The importance of establishing SLA and the parties it governs, e.g. service providers and clients.  **<Purpose>**  The purpose is to create a backup that allows the business to continue its operation after a system failure or incident.  **<Scope>**  It includes the services, products, and support provided that are covered under the agreement.  **<Terms and conditions>**  The terms for which the agreement is effective for, the conditions for adherence, termination and renewal, and exceptions.  **<Service Level>**  The service level performance criteria of what the service provider should achieve in order to meet the defined service level, e.g. system uptime should be > 99%.  **<Monitoring and reporting>**  The form, mode, and frequency of monitoring that the service provider shall provide to the client in order to report and exemplify that the service levels are being met. If the service provider fails to meet the defined service level, a detailed report on the root cause and follow up actions should be reported as well.  **<Indemnification>**  This is used to indemnify the client from and against any liabilities arising from the negligence of the service provider.  **<Acknowledgement>**  Both parties are to provide a sign off with the name, designation, company name and date to acknowledge they have understood and agreed to whatever was written in the agreement.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 22 — Template for Key Risk Indicator (KRI)

|  |  |  |  |
| --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | |
| **Key Risk Indicator (KRI)** | **Risk Owner** | **Threshold** | **Result** |
| Metrics used in the measurement of risks | Personnel responsible for overseeing and ensuring the KRI does not go beyond the threshold | The maximum risk value that is within the organisation’s risk appetite | The actual value measured during the current period |
| e.g. % of network downtime | Infrastructure Team | e.g. <1% | e.g. 0% |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | |

## Appendix 23 — Template for Business Impact Analysis (BIA)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc. | | | | | | | | | |
| **System Name** | **Description** | **Location** | **Financial Impact** | **Customer Impact** | **Regulatory Impact** | **Total Impact** | **RTO** | **RPO** | **Rating** |
| Name of the system to carry out BIA | A brief description of the system, including the purpose, etc. | Where the system is currently located | What is the potential financial impact rating (1-5) | What is the potential customer impact rating (1-5) | What is the potential regulatory impact rating (1-5) | What is the aggregated impact (financial + customer + regulatory impact) | The acceptable duration of time that the system can experience downtime, without causing significant business impact | The acceptable amount of data that the system can afford to lose, without causing significant business impact | The criticality rating in terms of the timeframe to recover the system |
| e.g. Web Server | e.g. Used to host websites | e.g. Server room | e.g. 1 — <$1000 2 — $1000-$5000  3 — $5001-$10000  4 — $10001-$50000  5 — >$50000 | e.g. 1 — <10 customers 2 — 10-20 customers  3 — 21-30 customers  4 — 31-40 customers  5 — >40 customers | e.g. 1 — Low chance of violating non-legal binding regulations  2 — Some chance of violating non-legal binding regulations  3 — High chance of violating non-legal binding regulations  4 — Violated non-legal binding regulations  5 — Violated legal notice | e.g. 1+2+3= 6/30 | e.g. 3 hours | e.g. 12 hours | e.g. Low/Medium/High/Critical |
| **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. | | | | | | | | | |

## Appendix 24 — Template for Business Continuity Plan (BCP)

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  The importance of business continuity and the organisation's system of procedures to restore critical business functions in the event of an unplanned disaster.  **<Purpose>**  The purpose is to document the requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve business-critical functions to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.  **<Scope>**   1. Persons/groups covered by the plan (e.g. Employees) 2. Geographic locations/facilities covered by the plan (e.g. all offices, head office, data centres) 3. Activities/process to be recovered   **<Roles and Responsibilities>**  The roles and responsibilities of the personnel for managing the disruptive incident, and who is authorised to perform certain activities in case of a disruptive incident (e.g. activation of the plans, urgent purchases, communication with media)  **<Activation Criteria>**  When the plan can be activated, and the method of activation. This would also include the conditions that need to exist to deactivate the plan. (e.g. specific thresholds of any prioritised operations which require the activation of the BCP).  **<Communication Details>**  The communication process of who to inform. This would also include the communication channel and contact details of the relevant stakeholders.  **<Continuity Strategies>**  Description of step-by-step actions and responsibilities for recovering manpower, facilities, infrastructure, software, information, and processes, including interdependencies and interactions with other activities and external interested parties.  **<Continuity Scenarios>**  Different scenarios which may activate the plan and the step-by-step procedure of how the BCP will be activated for each scenario.  **<Continuity Test>**  Performing a business continuity test which includes the frequency, testing procedures, and how the testing outcomes should be documented and reported to the senior management.  **<Review Schedule>**  The frequency when the plan should be reviewed and signed off, with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 25 — Template for Disaster Recovery Plan (DRP)

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  The importance of disaster recovery, and recovery of the organisation’s IT infrastructure and IT services, within the set recovery time objective.  **<Purpose>**  The purpose is to define how the organisation will recover its IT infrastructure and IT services within set deadlines, in the case of a disaster or other disruptive incidents.  **<Scope>**  Description of procedures to recover all business-critical services in the case of a disaster or other disruptive incidents.  **<Roles and Responsibilities>**  The roles and responsibilities of the disaster recovery team for managing the recovery of systems and data in an event of a disaster.  **<Activation Criteria>**  When can the plan be activated, and what is the method of activation? This would also include the conditions that need to exist to deactivate the plan. (e.g. specific thresholds of any prioritised operations which require the activation of DRP).  **<Communication Details>**  The communication process of who to inform. This would also include contact details of the relevant stakeholders.  **<Recovery Strategies>**  Description of step-by-step actions and responsibilities for recovering manpower, facilities, infrastructure, software, information, and processes, including interdependencies and interactions with other activities and external interested parties.  **<Recovery Test>**  Performing a disaster recovery test which includes the frequency, testing procedures, and how the testing outcomes should be documented and reported to the senior management.  **<Recovery Scenarios>**  Different scenarios which may activate the plan and the step-by-step procedure of how the DRP will be activated for each scenario.  **<Review Schedule>**  The frequency of when the plan should be reviewed and signed off with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. date, name, designation, signature, etc. |

## Appendix 26 — Template for Crisis Management Plan (CMP)

|  |
| --- |
| *\*Disclaimer: This template is a sample reference and is not meant to be used as it is. Enterprises should tailor it to fit their specific needs/requirements before using it.*  **<Change Log>**  A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.  **<Overview>**  The importance of overall coordination of an organisation's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimising damage to the organisation's profitability, reputation, or ability to operate.  **<Purpose>**  The purpose is to provide guidance to the organisation in the management of crisis response and recovery in the event of a crisis/major business disruption.  **<Scope>**  Description of procedures to manage crisis response and recovery in the event of a crisis/major business disruption.  **<Roles and Responsibilities>**  The roles and responsibilities of the Crisis Management Team (CMT) for managing a crisis.   1. CMT Chairperson:    * Declare crisis activation and standing down    * Crisis command and control    * Decision-making (e.g. approvals of communication and appointment of spokesperson) 2. Head of Finance:    * Analyse and brief CMT on financial impact of incident and organisation’s overall finance position    * Report and monitor financial losses and expenditure of crisis and recovery efforts    * Advise CMT on financial matters 3. Head of Operations:    * Evaluate impact on technology and operations    * Advise on overall business impact and recovery of business 4. Strategic Communications:    * Advise on corporate communication strategies    * Advise on key holding statements/messages to be included in mass communication with the press, public, customers, and other interested stakeholders 5. Legal and Compliance    * Advise on potential legal and compliance issues arising from the crisis and recommend an appropriate course of action    * Inform and manage relevant regulators 6. Human Resource    * Advise on HR/employees issues arising from the crisis    * Work with Strategic Communications to communicate with internal employees 7. IT/Security Representative    * Provide IT/cyber expertise and/or advice to the planning process, and lead the IT crisis response   **<Criteria for Crisis>**  When the plan can be activated, and what the method of activation is. This would also include the conditions that need to exist to deactivate the plan. (e.g. specific thresholds of any prioritised operations which require the activation of the CMP.)  **<Crisis Communication Protocols>**  The communication process of who to inform (e.g. customers and regulators). This would also include communication statements, a designated spokesperson, and the contact details of the relevant stakeholders.  **<Crisis Test>**  Performing crisis management which includes the frequency, testing procedures, and how the testing outcomes should be documented and reported to senior management.  **<Review Schedule>**  The frequency when the plan should be reviewed and signed off with the version, date, and signature by senior management.  **<Sign Off>**  The sign offs from the management approving this policy, e.g. de, name, designation, signature, etc. |

1. The asset tag should provide unique identification for each of the assets, e.g. it can be concatenated with acronyms of the asset type, department prefix, and a running number to form a unique identifier. [↑](#footnote-ref-1)