POLICY TEMPLATE

The policy template provides general guidance for Healthcare Institutions (HCI) to adapt based on your operational needs. HCIs should review the Healthcare Cybersecurity Essentials (HCSE) issued by the Ministry of Health and translate them into policies for the organisation. Examples provided in the policy template are non-exhaustive. Licensees who use this policy template should exercise judgement and adjust it accordingly based on your operational needs.

Policies provide written guidance explaining processes and procedures needed to be undertaken to comply with HCSE. This written guidance should be unambiguous and clear.

The checklist below serves as a guide for licensees' internal use to ensure that the policies put in place is effective:

Key Aspects of an Effective Written Security Policy	**Yes (✓)**
(a) The policy should be endorsed by relevant personnel with organisational authority to effect change and ensure compliance (e.g. head of organisation, chief information security officer, licensees under the Private Hospitals and Medical Clinics Act).	
(b) The policy should be communicated to and discussed with all staff (including new staff) and IT vendors regularly to remain relevant.	
(c) The policy should be easily accessible by staff who are accessing and using an organisation's IT assets and resources.	
(d) The policy should be periodically reviewed to ensure they are current and updated when changes are made to the processes in your practice or to HCSE or relevant legislation.	
(e) The policy should be re-issued and communicated all staff and IT vendors especially when updated substantially.	
(f) The version number of the policy should be updated when changes are made to facilitate tracking and communication to staff and IT vendors.	

[Insert Policy title]
Your policy title should reflect the subject of the policy and be written in plain language.
E.g. Cybersecurity policy

Current as of: [Insert date of last revision]

Endorsed by: **[Insert name…should be by someone of enough seniority]**

A. Introduction

The introduction to your policy should outline:

- *What kind of information the policy provide?*

E.g. The policy establishes the processes for maintaining accounts to all systems, defines rules for accessing into administrator account and establishes guidelines for account creation and removal. The policy also set out other requirements to protect patients' personal data and medical record.

- *who is responsible for implementing this policy?*
  E.g. head of IT department or clinic manager

B. Purpose and objectives

This section should explain why the policy is required and what it addresses in the organisation.
E.g. The policy set out a clear requirement on the DOs and DON'Ts that all staff in the organisation must abide to in order to protect the information create, process and store in the IT systems for the provision of healthcare services. All staff are to ensure they read, understand and comply with the policies and be aware of their responsibilities and obligations as users and administrators of the IT systems.

C. Scope

This section should describe who the policy applies to and what activities the policy covers. HCI should also determine what action will be taken if this policy is breached and outline this as part of the policy scope. HCI should also have a process for recording the understanding and agreement of all staff and IT vendors.

*E.g. This policy applies to all personnel of **[HCI's name]**, including licensees, clinic manager, clinic assistant, pharmacist, interns, IT vendors and any personnel who is authorised to access **to [HCI's name]** IT systems. The policy covers any activities relating to accessing **[HCI's name]** IT systems to perform their work.*

Violation of these policies could result in one of the following:

- disciplinary action such as warning letter
- termination of employment/contract
- staff or IT vendors being held personally liable for damages caused by any violations of this policy

All staff and IT vendors are required to confirm they have understood and agree to comply with this policy.

D. Definitions

This section should define words or terms in the policy that may not be commonly understood, including acronyms and any technical information.

E. Policy content

This section should outline the actual policy information. The content should be structured in a concise and direct manner so that the policy can be easily followed, implemented and enforced.

Ensure the policy content clearly states what action needs to be taken and who is responsible for taking this action.

E.g.
IT asset Management Policy

- *[IT manager/clinic manager] creates and maintains an inventory of endpoints, including the number of servers, storage devices, routers, desktops, laptops and tablets etc.*

- *[IT manager/clinic manager] creates and maintains an inventory of software and applications, including clinical management and electronic medical records systems, accounting and HR software, Word and Excel etc.*
- *[IT manager/clinic manager] updates the lists [quarterly] or on as needed basis (where applicable) to reflect the current inventory of endpoints, software and applications.*

Administrator, user accounts management and password policy

- *[IT manager/clinic manager] reviews the access rights accorded to privileged administrator accounts and user accounts (with limited privileges) on [frequency].*
- *Users are responsible for all activities performed with their user accounts. Passwords must not be shared or revealed to anyone else besides the authorised users.*
- *Users with administrator privileges should only use their administrator account when required, and not for any personal use or accessing external websites.*
- *[IT manager/clinic manager] reviews the access log of administrator account [frequency] to determine if systems have been breached and flag out possible inappropriate accesses*
- *[IT manager/clinic manager] authenticates the identity of new users before providing them with account, username and password details.*
- *[IT manager/clinic manager] maintains a list of accounts created and reviews all accounts and account privileges [frequency] to ensure that access and account privileges are commensurate with job functions, need-to-know, and employment status.*
- *[IT manager/clinic manager] instructs IT vendor to disable all accounts which are unused, misused or compromised. [IT manger/clinic manger] instructs IT vendor to recover the disabled account only after relevant checks are completed.*
- *[IT manager/clinic manager] instructs IT vendor to remove a user's account within [X days/weeks] after a user leaves the organisation.*

Policy on security patches

- *Patching should be done based on the criticality of the patches. For critical patches or patches for critical application, the updates should be done within 3 days by <which administrator>.*
- *[IT manager/clinic manager] upgrades all End of Support (EOS) machines and Operating System through tech refresh to ensure that machines and system can support the latest security patches.*

Policy on monitoring of audit logs

- *[IT manager/clinic manager] ensures that the logging of user activities and security events (login, logout and failed logins) of accounts are set up for audit trails.*
- *[IT manager/clinic manager] reviews the audit logs on [frequency] for unauthorised access and unusual or inappropriate activity and report to [relevant personnel and authority].*
- *Audit logs are only accessible by [IT manager/clinic manager].*

Policy on backup

- *[IT manager/clinic manager] performs frequent and regular [frequency] backups of all critical data and systems in a secure manner.*
- *[IT manager/clinic manager] tests backups on [frequency] to ensure they are usable during an emergency or ransomware attack.*

Policy on outsourcing and vendor management

- *[Clinic manager] checks and understands from the third-party vendor on how the patient and corporate data is processed, transferred and stored in the third-party software/device.*
- *[Clinic manager] checks and understands the safeguards the third-party vendors have in place to secure the third-party software/device.*

- *[Clinic manager] checks and understands the delineation of roles and responsibilities in the event of an incident and breach before entering into contractual agreement with the third-party vendors.*
- *[Clinic manager] subscribes to security-related alerts published by vendors for the third-party software and devices used in the clinic.*
- *In the event that the clinic engages an IT service provider to manage its network and systems, [clinic manager] checks and understands the services and security practices of the providers. [Clinic manager] requests for regular vulnerability reports and updates about security issues for systems the IT service providers are managing for you.*

Policy on cybersecurity awareness among users

- *[Clinic manager] ensures that users who access systems and data must undergo suitable training and awareness programme.*
- *[Clinic manager] updates the training and awareness programme regularly to ensure the content is relevant.*
- *[Clinic manager] puts up suitable signages and/or posters to remind users on e.g. securing passwords, logging off/shutting down system and application after use and use of trusted network connection and website.*
- *[Clinic manager] ensures any updates to organisation's internal cybersecurity policies are communicated to all staff (including new staff).*

Policy on cybersecurity incident reporting

- *[Clinic manager] ensures that all users are familiar on how and who to report the incident report or any suspicious activity to within the organisation (e.g. clinic manager, head of organisation or specific staff appointed by the head of organisation to handle incident).*
- *[Clinic manager] prepares contingency plans (e.g. containing and assessing the breach and recovering critical data from backup) for possible cybersecurity incidents and runs regular stimulation exercise on [frequency] to better prepare staff in responding to cybersecurity incidents.*
- *[Clinic manager] reports the cybersecurity incident to SingCERT, PDPC or other relevant authority based on your obligations under prevailing legislative or regulatory requirements.*

F. Related Policies and Processes

This section should list down the policies and processes written by your HCIs that are relevant to the staff and IT vendor

E.g.

- *Internet and email Policy*

G. Exception

This section should provide situations (if any) where exceptions to this policy would be permitted

E.g. Exceptions to this policy will only be allowed with written approval by head of organisation (i.e. endorser of this policy).

H. Policy review statement

This section should provide a statement regarding the regular review of the policy. You can set a specific review date for your policies

E.g. This policy will be reviewed annually to ensure it reflects the current processes and procedures of ***[HCI's name]*** *and current legislation requirements.*