Recommended Minimum Policy Requirement - FinCSIRT

0	**Common criteria for every policy**	
	Minimum topics to be covered within the policy	• Policy purpose and Scope should be mentioned at the top of the document. • Roles and responsibilities for conduct and maintenance of the document • Document review date and versioning should be maintained and clearly mentioned on the document • Policy compliance auditing methodology • Exceptions to the policy should be mentioned • Non-compliance and policy violation must be addressed in each policy with penalties • Related procedures plus compliance laws/regulations, standards, best practices and other reference documents should be clearly mentioned • Each policy/procedure should carry its own Key Performance Indicators (KPI), Key Risk Indicators (KRI), Key Control Indicators (KCI)

1	**Policy Name:**	Information Security Policy (ISP)
	Description	An organization's information security policy is a high-level document that communicate the business goals and objectives on its information security to its employees.

	Minimum aspects to be covered under the policy	• Organizational information security strategy and maintenance
		  ○ Management commitment statement to support the information security strategy of the organization
		  ○ Responsibility of CISO, ISO and Information security steering committee
		• Classification of Information/data
		  ○ Information classification levels and their definitions/criteria
		  ○ Classification Tagging mechanism
		• Information Sharing and Information disclosure
		  ○ List of External Information sharing accepted parties and types of information
		  ○ Required controls aligning information classification policy
		  ○ External data/information sharing requirement (E.g.: NDA)
		• User and System classifications
		  ○ Access control and granting procedure
		• Reference Sub Policies, Standards, Regulations, Best Practices and Guidelines

2	**Policy Name:**	Acceptable Use Policy (AUP)
	Description	AUP stipulates the acceptable use of the organizational information/data and IT assets by an employee.

	Minimum aspects to be covered under the policy	• What is the acceptable use of the organizational information/data and IT assets
		  ○ List/scope of assets that are covered by the AUP
		  ○ Acceptable levels of uses that each assets are usable for the employees
		  ○ Responsibility of the employee with the use of information/data and IT assets
		Sample policy points to use:
		→ *If the organization is monitoring the resources usage for audit and security purposes, it should be noted.*
		→ *All devices (mobiles, tabs) owned by employees should adhere to organizational policies and procedures if used to access, process or transmit organizational information. (If require have a separate BYOD policy)*
		→ *Usage of organizational identities (email, designation) outside of the job scope is not accepted unless it is pre-authorized and those opinions or expressions are strictly their own.*
		→ *Employees should be informed that organizational resources should only be used for the extent that it is authorized and necessary to fulfill their assigned job duties. (If require have a separate COPE policy)*

3	**Policy Name:**	Access Control Policy (ACP)
	Description	The ACP outlines the access granting and revoking mechanism, and user responsibilities accessing the organization's data and information systems.
	Minimum aspects to be covered under the policy	• Access requesting, granting and revocation procedure • Who is authorized to grant the access • Procedure for the revocation • Procedure for access granting and revoking announcements • List of access categories aligning data classification levels • List of authentication mechanisms required under each access category and its minimum configuration policy (E.g.: Password complexity, OTP, biometrics, tokens…etc.) • Access sharing policy of the organization • Access granting for 3rd party non-employees/vendors • Temporary access policy of the organization • Remote access policy of the organization • Use of superuser/all access roles/accounts (Recommended of using personally identifiable accounts) • Central and Local user account management policy of the organization • Monitoring mechanism • Availability requirement of the Logs; its Retention time period and mechanism • Access permissions for the Logs

4	**Policy Name:**	Change Management Policy (CMP)
	Description	Change management policy refers to a formal process for making changes to Information Systems.

	Minimum aspects to be covered under the policy	• Change request, approve and confirm procedure
		• Change approval procedure
		• Emergency change procedure
		  ○ Classification of emergency change
		  ○ Emergency change approval, implementation, testing and confirmation procedure
		• Change issue tracking/monitoring procedure
		• Change implementation and testing procedure
		• Backup requirements for changes

	• Rollback procedure

5	**Policy Name:**	Remote Access Policy
	Sub Policy of	Access Control Policy (ACP)
	Description	The remote access policy is a document which outlines and defines acceptable methods of remotely connecting to an organization's internal networks.
	Minimum aspects to be covered under the policy	• List systems that allow remote access directly from internet and the medium/services • List of users (Internal and External) allowed to connect to the organizational network using remote connections and the medium (If location specific, it should be mentioned) • Access control/Authentication mechanisms which are needed to connect to the organization remotely • Access request, approval and granting procedure for required remote access • Access duration and access revocation policy and procedures • Remote device suitability criteria's for accessing the network remotely • Access logs and audit logs retention and management • Session timeout and session count per server/system

6	**Policy Name:**	Email/Communication Policy
	Description	A company's email policy is a document that is used to formally outline how employees can use the business' chosen electronic communication medium
	Minimum aspects to be covered under the policy	• e-mail account creation, deletion and disabling policy • Organizational e-mail ethics and guidelines • e-mail content filtering policy regarding malicious /spam contents • e-mail retention and archiving policy of the organization • e-mail subject and content requirement (E.g.: Email Signature, classification labelling, disclaimer…etc.) • e-mail classification policy which aligns with the information classification and sharing policy • External applications and web email accessing policy

7	**Policy Name:**	Business Continuity and Disaster Recovery Policy (BCP and DR Policy)
	Description	The BCP and DR policy will coordinate efforts across the organization and will use the disaster recovery plan to restore hardware, applications and data deemed essential for business continuity. BCP's are unique to each business because they describe how the organization will operate in an crisis
	Minimum aspects to be covered under the policy	• Identification of the business critical systems/processes criteria • Business Impact Analysis conducting criteria • RTO and RPO defining criteria • DR requirement • Data backup and restoration policy of the organization • Incident response policy of the organization • Roles and responsibilities, line of authority , succession management and interactions with external contractors and vendors should be available • BCP and DR Testing drills and verification • BCP and DR switch criteria • Training requirements • Lesson learn integration criteria • Communication and escalation plan • Minimum SLA requirements with third-party vendors/suppliers/service providers

8	**Policy Name:**	Incident Response (IR) Policy
	Sub Policy of	BCP & DR Policy
	Description	The incident response policy is an organized approach to how the company will manage an incident and remediate the impact to operations.
	Minimum aspects to be covered under the policy	• Incident identification procedure • Classification of the Incident with criticality definition • IR team responsibilities • IR procedure • IR communication procedure and Call Tree • Evidence obtaining and preservation procedure • Incident Escalation and sharing procedure to CSIRT/CERT and other compliance/regulatory bodies • Lesson learnt integration procedures

9	**Policy Name:**	Backup, Restore, Retention and Disposal Policy
	Sub Policy of	BCP & DR Policy
	Description	This document will describe the data backup policy and procedures for backup, verify and restore so that the organization could recover from. Further, it defines the procedures and policy for data and configuration storing, retention, deletion and lifecycle management so that it will be aligned with organizational security strategy
	Minimum Topics to be covered	• Backup Storage requirements (Encryption etc.) • Backup retention period and disposing mechanism • List of source and backup locations • Backup frequency and Backup type • Restoration procedure • Testing procedure • Issue escalation procedure

10	**Policy Name:**	Clean desk policy

Description	A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation

Minimum aspects to be covered under the policy	• Workstation lockout mechanism policy of the organization
	• Sensitive information protection mechanism which are on physical forms
	  ○ Work area disciplines
	  ○ Physical information storage requirements
	  ○ Physical information disposal requirements
	• Should define the locations that this policy will be applied to

11

Policy Name:	Digital Signature Policy
Description	Defines the requirements for when a digital signature is considered an accepted means of validating the identity of a signer in electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization.
Minimum aspects to be covered under the policy	• Digital signing key creation, deletion and disabling policy • Digital signature applicable instance list • Signer responsibilities over digital signature usage • Signing software requirements • Digital signing key Protection requirements • Recipient responsibilities for digital key verification • Digital signing key revocation procedures

12

Policy Name:	Common security configuration policy
Description	This policy will cover the minimum security configuration requirement for applications, servers and devices
Minimum areas to be covered	• Time synchronization criteria policy of the organization • Transport layer of security (TLS) and minimum version • Services exposure requirement (E.g.: enable only the required services…etc.) • Authentication and authorization should be managed • Access request, granting and revocation policy of the organization • Configuration Backup procedure policy of the organization • Policy on superuser account usage • Policy on access to applications, servers and devices management • Jump server usage policy

13

Policy Name:	Media Dispose Policy
Description	This policy governs the requirements and procedures for secure media disposal
Minimum areas to be covered	• Media disposal procedure • User responsibilities on handing media for disposal • Identification criteria for media disposal mechanism • Log maintenance for media disposal • Data disposal verification policy • Conditions which the medium should be designated for disposal

14

Policy Name:	Information Sharing Policy
Description	This policy governs the requirements and procedures for information/data sharing internally and externally
• **Minimum areas to be covered**	• List of External Information sharing accepted parties and types of information • External communication and sharing information/data authorization procedure • Required controls aligning information classification policy • External data/information sharing requirement (E.g.: NDA)