#	Policy / Procedure	Description
1	**Asset Management**	This policy describes the activities required to perform Asset Management (e.g. Identify and manage business purposes).
2	**Business Environment**	This policy describes the organizational cyber security roles and risk management decisions
3	**Governance**	This purpose is to establish organizational policies, process and procedures for information security and risk management.
4	**Risk Assessment**	This policy's purpose is to identify the organizational asset vulnerabilities and cybersecurity risk to operations.
5	**Risk Management Strategy**	This policy describes organizational risk tolerance and established operational risk decisions.
6	**Access Control**	The purpose is to provide management for limited access to facilities and organization assets.
7	**Awareness and Training**	The purpose is to provide cyber security awareness and training to organizational personnel covering their jobs and responsibilities.
8	**Data Security**	The purpose is to provide risk strategy to ensure the confidentiality, integrity, and availability (CIA) of information assets.
9	**Information Protection Processes and Procedures**	The purpose is to maintain policies, processes, and procedures to manage protection of information systems and assets.
10	**Maintenance**	The purpose is to maintain policies and procedures for the maintenance and repairs of organizational assets
11	**Protective Technology**	The purpose is to provide Technical security solutions to ensure the security and protection of systems and organizational assets.
12	**Anomalies and Events**	This policy ensure to detect anomalous activities and events in a timely manner.
13	**Security Continuous Monitoring**	The purpose is to monitoring the physical environment, information system and assets at discrete intervals to identify cybersecurity events.
14	**Detection Processes**	The purpose is to provide awareness on anomalous events and test detection activities.
15	**Response Planning**	The purpose is to maintain response plan to ensure timely response to detected cybersecurity

#	Policy / Procedure	Description
		events.
16	**Communications (Respond)**	The purpose is to coordinate response activities with stakeholders consistently to achieve broader cybersecurity situational awareness.
17	**Analysis**	The purpose is to conduct analysis to understand response and recovery activities.
18	**Mitigation**	The purpose is to perform activities to mitigate incident and newly identified vulnerabilities.
19	**Improvements (Respond)**	The purpose is to the improvement of response plan by incorporating lessons learned from all response activities.
20	**Recovery Planning**	This policy ensures timely restoration of systems or assets affected by cybersecurity events.
21	**Improvements (Recover)**	The purpose is to the improve recovery planning and processes by incorporating lessons learned.
22	**Communications (Recover)**	This purpose is to Communicate recovery activities to internal stakeholders and repair the reputation after an event.