Title :	APAR – CIS Policy
Effective from:	27th December 2016
Released by:	President Strategy & Projects
Date of Amendment:	24th February 2023
Version:	v2/ 2023

Corporate Information Security Policy

Version: 2.0

Document No.: CISP-SM-01

Corporate Information Security Policy

"The Information assets are critical to the success of our business. It is essential to ensure the confidentiality, integrity and availability (CIA) of the information assets of our company by using the most appropriate processes and technology."

Objective

Objective of Corporate Information Security Policy is to govern the set of policies and procedures that need to be implemented and followed to ensure that the Information assets of the company remain secure by being available, confidential and in a state where they would be reliable and accurate.

Corporate Information Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security or Cyber security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

APAR's Corporate Information Security policies covers the following areas

1. Network security - the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

2. Application security - focuses on keeping software and devices free of threats. A compromised application could provide access to the data it is designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

3. Information security - protects the integrity and privacy of data, both in storage and in transit.

4. Operational security - includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

5. Disaster recovery and business continuity - define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

6. End-user education - addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users on safe and acceptable usage practices is vital for the security of any organization.

The above aspects are covered in a set of policy documents organised into 6 Apex Policies and 25 Sub Policies.

A summary of the available policies are listed below and the details of each policy is accessible via links provided against the description

	Policy Name	Policy No.
	APEX Policy	
1	Corporate Information Security Policy	CISP-SM-01
2	Information Security Management Framework	ISMS-SM-01
3	Information Asset classification Policy and Procedure	ISMS-SM-02
4	Information Security Sustenance Policy and Procedure	ISMS-SM-03
5	Information Security Organization Policy	ISMS-SM-04
6	Information Security Risk Management Procedure	ISMS-SM-05
	ISMS Sub Policy and Procedures	
1	Acceptable Usage Policy & Procedure	ISMS-SM-06
2	Access Control Policy for Logical & Physical Network	ISMS-SM-09
3	Application Development, Security and Operation	ISMS-SM-19
4	Backup and Restore Policy	ISMS-SM-10
5	BYOD (Bring Your Own Device) Policy & Procedure	ISMS-SM-39
6	Capacity Management Policy & Procedure	ISMS-SM-41
7	Change Management Policy & Procedure	ISMS-SM-11
8	Clear Desk and Clear Screen Policy	ISMS-SM-12
9	Compliance Policy	ISMS-SM-22
10	Data Retention, Storage & Disposal of Media, Records	ISMS-SM-17
11	Document Encryption Procedure	ISMS-SM-37
12	Electronic Mail Security Policy Procedures	ISMS-SM-24
13	Information Security Continuity Policy	ISMS-SM-35
14	Information Security Incident Management Policy	ISMS-SM-20
15	Internet Policy and Procedures	ISMS-SM-26
16	IT Hardware & Software License Management Policy	ISMS-SM-16
17	Malware Security Policy	ISMS-SM-08
18	Mobile Device Security Policy	ISMS-SM-23
19	Network Security Policy and Procedure	ISMS-SM-30
20	Outsourced Services Security Policy & Procedure	ISMS-SM-25
21	Password Policy & Procedure	ISMS-SM-18

	Policy Name	Policy No.
22	Patch Management Policy & Procedure	ISMS-SM-38
23	Personnel Security Policy and Procedure	ISMS-SM-40
24	Physical Security Policy	ISMS-SM-13
25	Virtual Private Network Policy	ISMS-SM-15