Statement of Applicability

Theme	Annex A Control	Control Objective	Control Applied?	Control Owner	Implentation Date	Date of Last Assessment
Organisational Controls						
	A.5.1 – Information Security Policies	Define, approve, publish, and communicate security policies.	Yes	CISO & GM	1/1/25	N/A
	A.5.2 – Roles and Responsibilites	Clearly define information security duties for key roles.	Yes	CISO & GM	1/1/25	N/A
	A.5.4 – Management Direction for Information Security	Provide management direction and support for information security.	Yes	GM	1/1/25	N/A
People Controls						
	A.6.2 – Terms and Conditions of Employment		Yes	HR	1/1/25	N/A
	A.6.3 – Information Security Awareness, Education and Training		Yes	CISO & SOC	1/1/25	N/A
	A.6.7 – Remote Working	Remote workers accessing policy systems need endpoint hardening and VPN enforcement.	Yes	CISO, NOC & SOC	1/6/25	N/A
	A.6.8 – Information Security Event Reporting					
Physical Controls						
	A.7.2 – Physical Entry Controls	100 % of restricted areas require badge authentication.	Yes	HR	1/1/25	N/A
	A.7.3 – Securing Offices, Rooms and Facilities	Security measures are in place for facility access.	Yes	HR & GM	1/1/25	N/A

Technological Controls						
	A.8.1 – User Endpoint Devices	Secure configuration and protection of laptops, desktops, and mobile devices.	Yes	NOC & Infra	1/1/25	N/A
	A.8.2 – Restrict and manage privileged accounts.	Servers and desktops require admin accounts; misuse could lead to critical data compromise.	Yes	Infra	1/1/25	N/A
	A.8.9 – Configuration Management	Apply standard configurations to IT assets and track changes.	Yes	SD	1/1/25	N/A
	A.8.13 – Ensure backup and restore procedures are effective.	Annual restore tests are part of security objectives; critical for business continuity.	Yes	NOC	1/1/25	N/A
	A.8.16 – Monitoring Activities	Monitor systems and networks for abnormal activity and unauthorized access.	Yes	SOC	1/1/25	N/A