Oneflow Statement of Applicability (External). Version 1.1. Date: June 13, 2024.

#	Name of control	Relevant/Applicable?	Implementation status
5.1	Policies for information security	Yes	Done
5.2	Information security roles and responsibilities	Yes	Done
5.3	Segregation of duties	Yes	Done
5.4	Management responsibilities	Yes	Done
5.5	Contact with authorities	Yes	Done
5.6	Contact with special interest groups	Yes	Done
5.7	Threat intelligence	Yes	Done
5.8	Information security in project management	Yes	Done
5.9	Inventory of information and other associated assets	Yes	Done
5.10	Acceptable use of information and other associated assets	Yes	Done
5.11	Return of assets	Yes	Done
5.12	Classification of information	Yes	Done
5.13	Labelling of information	Yes	Done
5.14	Information transfer	Yes	Done
5.15	Access control	Yes	Done
5.16	Identity management	Yes	Done
5.17	Authentication information	Yes	Done
5.18	Access rights	Yes	Done
5.19	Information security in supplier relationships	Yes	Done
5.20	Addressing information security within supplier agreements	Yes	Done
5.21	Managing information security in ICT supply chain	Yes	Done
5.22	Monitoring, review and change management of supplier services	Yes	Done
5.23	Information security for the use of cloud services	Yes	Done
5.24	Information security incident management planning and preparation	Yes	Done
5.25	Assessment and decision on information security events	Yes	Done
5.26	Response to information security incidents	Yes	Done
5.27	Learning from information security incidents	Yes	Done
5.28	Collection of evidence	Yes	Done
5.29	Information security during disruption	Yes	Done
5.30	ICT readiness for business continuity	Yes	Done
5.31	Legal, statutory, regulatory and contractual requirements	Yes	Done
5.32	Intellectual property rights	Yes	Done
5.33	Protection of records	Yes	Done
5.34	Privacy and protection of PII	Yes	Done
5.35	Independent review of information security	Yes	Done
5.36	Compliance with policies, rules and standards for information security	Yes	Done
5.37	Documented operating procedures	Yes	Done
6.1	Screening	Yes	Done
6.2	Terms and conditions of employment	Yes	Done
6.3	Information security awareness and training	Yes	Done
6.4	Disciplinary process	Yes	Done

6.5	Responsibilities after termination or change of employment	Yes	Done
6.6	Confidentiality or non-disclosure agreements	Yes	Done
6.7	Remote working	Yes	Done
6.8	Information security event reporting	Yes	Done
7.1	Physical security perimeters	Yes	Done
7.2	Physical security	Yes	Done
7.3	Securing offices, rooms and facilities	Yes	Done
7.4	Physical security monitoring	Yes	Done
7.5	Protecting against physical and environmental threats	Yes	Done
7.6	Working in secure areas	Yes	Done
7.7	Clear desk and clear screen	Yes	Done
7.8	Equipment siting and protection	Yes	Done
7.9	Security of assets off-premises	Yes	Done
7.10	Storage media	Yes	Done
7.11	Supporting utilities	Yes	Done
7.12	Cabling security	Yes	Done
7.13	Equipment maintenance	Yes	Done
7.14	Secure disposal, or re-use of equipment	Yes	Done
8.1	User endpoint devices	Yes	Done
8.2	Priviliged access rights	Yes	Done
8.3	Information access restriction	Yes	Done
8.4	Access to source code	Yes	Done
8.5	Secure authentication	Yes	Done
8.6	Capacity management	Yes	Done
8.7	Protection against malware	Yes	Done
8.8	Management of technical vulnerabilities	Yes	Done
8.9	Configuration management	Yes	Done
8.10	Information deletion	Yes	Done
8.11	Data masking	Yes	Done
8.12	Data leakage prevention	Yes	Done
8.13	Information backup	Yes	Done
8.14	Redundancy of information processing facilities	Yes	Done
8.15	Logging	Yes	Done
8.16	Monitoring activities	Yes	Done
8.17	Clock synchronization	Yes	Done
8.18	Use of privileged utility programs	Yes	Done
8.19	Installation of software on operational systems	Yes	Done
8.20	Network security	Yes	Done
8.21	Security of network services	Yes	Done
8.22	Segregation of networks	Yes	Done
8.23	Web filtering	Yes	Done
8.24	Use of cryptography	Yes	Done
8.25	Secure development life cycle	Yes	Done
8.26	Application security requirements	Yes	Done

8.27	Secure systems architecture and engineering principles	Yes	Done
8.28	Secure coding	Yes	Done
8.29	Security testing in development and acceptance	Yes	Done
8.30	Outsourced development	Yes	Done
8.31	Separation of development, test and production environments	Yes	Done
8.32	Change management	Yes	Done
8.33	Test information	Yes	Done
8.34	Protection of information systems during audit testing	Yes	Done