Statement of Applicability

#	ID	Control Name	Applicability	Implementation Status	Explanatory Notes
A.5 Organizational Controls					
1	A.5.1	Policies for information security	Applicable	Implemented	The organization has established a formal Information Security Policy approved by top management. The policy defines objectives, principles, and responsibilities for information security and is communicated internally. The policy is reviewed periodically and aligned with the ISMS scope and risk management results.
2	A.5.2	Information security roles and responsibilities	Applicable	Implemented	Information security roles and responsibilities are formally defined and assigned, including the roles of Security Officer, IT Manager, and Data Protection Officer (DPO). Responsibilities are documented in internal regulations and job descriptions and are supported by management commitment.
3	A.5.3	Segregation of duties	Applicable	Implemented	Segregation of duties is implemented to reduce the risk of unauthorized or unintentional modification or misuse of information assets. Critical responsibilities are divided between different roles where feasible, taking into account the size and structure of the organization.
4	A.5.4	Management responsibilities	Applicable	Implemented	Top management actively supports the ISMS and ensures that information security requirements are integrated into organizational processes. Management responsibilities related to information security are formally documented and communicated.
5	A.5.5	Contact with authorities	Applicable	Implemented	The organization maintains defined procedures for contacting relevant authorities in the event of information security incidents, including data protection incidents. Responsibilities and escalation paths are documented.
6	A.5.6	Contact with special interest groups	Applicable	Implemented	The organization monitors relevant information security sources, professional groups, and vendor communications to stay informed about emerging threats, vulnerabilities, and best practices applicable to its environment.
7	A.5.7	Threat intelligence	Applicable	Implemented	Threat intelligence is obtained through external sources such as NBU, cloud service providers, and security advisories. Relevant threat information is considered as part of risk management and operational security activities.
8	A.5.8	Information security in project management	Applicable	Implemented	Information security requirements are integrated into project management activities. Security considerations are assessed during project planning and implementation phases in accordance with internal policies.
9	A.5.9	Inventory of information and other associated assets	Applicable	Implemented	An inventory of information assets is maintained, including systems, data, and supporting assets. Asset ownership and classification are defined and aligned with risk assessment results.
10	A.5.10	Acceptable use of information and other associated assets	Applicable	Implemented	Acceptable use of information and assets are defined in internal policies and communicated to employees. Compliance is supported through awareness activities and management oversight.
11	A.5.11	Return of assets	Applicable	Implemented	Procedures are in place to ensure the return or secure removal of organizational assets upon termination or change of employment.
12	A.5.12	Classification of information	Applicable	Implemented	Information is classified based on confidentiality, integrity, and availability requirements.
13	A.5.13	Labelling of information	Applicable	Partially implemented	Information assets are labelled in accordance with their classification where appropriate. Labelling supports correct handling of information and is applied in a proportionate manner, considering the organization's size and operational context.
14	A.5.14	Information transfer	Applicable	Implemented	Procedures for secure information transfer are defined and implemented.
15	A.5.15	Access control	Applicable	Implemented	Access control principles are defined in internal policies and implemented using role-based access mechanisms. Access rights are granted based on business needs, approved by management, and reviewed regularly.
16	A.5.16	Identity management	Applicable	Implemented	User accounts are created and managed by administrators in Microsoft Entra ID, with role-based assignments applied during the joiner–mover–leaver process and accounts removed from all repositories upon user departure.
17	A.5.17	Authentication information	Applicable	Implemented	Password complexity and expiration (approximately 180 days) are defined in internal policies, MFA is enforced for all users via Microsoft Entra ID, authentication data is protected using Microsoft default security controls, and shared user accounts are not permitted (only shared mailboxes linked to individual users).
18	A.5.18	Access rights	Applicable	Implemented	User access rights are assigned, modified and revoked in accordance with defined procedures. Access rights are reviewed periodically and upon changes in employment or role.
19	A.5.19	Information security in supplier relationships	Applicable	Implemented	Non-disclosure agreements are signed with suppliers as part of contractual arrangements, and supplier access to SharePoint is granted only when necessary, with limited permissions and restricted to specific documents;
20	A.5.20	Addressing information security within supplier agreements	Applicable	Implemented	Supplier contracts include non-disclosure obligations, data protection requirements, and defined responsibilities in case of information security incidents or breaches.
21	A.5.21	Managing information security in ICT supply chain	Applicable	Implemented	ICT supply chain risks are identified and managed as part of supplier risk management. Cloud service providers such as Microsoft (M365) and AWS are selected based on defined security and compliance criteria.
22	A.5.22	Monitoring, review and change management of supplier services	Applicable	Implemented	Supplier services are monitored and reviewed periodically to ensure continued compliance with security requirements. Changes affecting security are assessed and managed through defined change management processes.
23	A.5.23	Information security for use of cloud services	Applicable	Implemented	The organization uses cloud services as a primary delivery model. Information security requirements for cloud usage are defined, and responsibilities between the organization and cloud providers are clearly established and documented.
24	A.5.24	Information security incident management planning and preparation	Applicable	Implemented	Incident management processes are defined and documented. Roles, responsibilities and escalation paths are established to ensure timely and effective response to information security incidents.
25	A.5.25	Assessment and decision on information security events	Applicable	Implemented	Information security events are assessed to determine whether they constitute incidents. Assessment criteria and decision-making responsibilities are defined within the incident management process.
26	A.5.26	Response to information security incidents	Applicable	Implemented	Information security incidents are handled according to documented procedures. Response activities include containment, mitigation, recovery and communication, proportionate to the incident's impact.
27	A.5.27	Learning from information security incidents	Applicable	Implemented	Lessons learned from incidents are documented and reviewed. Findings are used to improve controls, procedures and awareness activities within the ISMS.
28	A.5.28	Collection of evidence	Applicable	Implemented	Procedures for the collection and preservation of evidence related to information security incidents are defined.
29	A.5.29	Information security during disruption	Applicable	Implemented	Information security requirements are maintained during disruptive events. Controls supporting confidentiality, integrity and availability are considered within business continuity and incident response processes.
30	A.5.30	ICT readiness for business continuity	Applicable	Implemented	ICT systems are prepared to support business continuity objectives. Business Impact Analysis (BIA) and continuity planning consider ICT dependencies and recovery requirements.
31	A.5.31	Legal, statutory, regulatory and contractual requirements	Applicable	Implemented	Relevant legal, statutory, regulatory and contractual information security requirements are identified, documented and monitored. Compliance obligations are considered within ISMS processes.
32	A.5.32	Intellectual property rights	Applicable	Implemented	Procedures are in place to ensure compliance with intellectual property rights. Use of licensed software and protection of proprietary information are addressed through policies and contractual controls.
33	A.5.33	Protection of records	Applicable	Implemented	Records are protected against loss, unauthorized access and improper disposal. Retention and protection requirements are defined in accordance with legal and business needs.
34	A.5.34	Privacy and protection of PII	Applicable	Implemented	Personal data and PII are protected in accordance with applicable data protection regulations. The role of DPO is formally established and privacy requirements are integrated into ISMS controls.
35	A.5.35	Independent review of information security	Applicable	Implemented	Independent reviews of information security are conducted through internal audits, management reviews and independent external penetration testings. Findings are documented and tracked to completion.
36	A.5.36	Compliance with policies, rules and standards for information security	Applicable	Implemented	Compliance with internal information security policies and standards is monitored. Non-compliance is addressed through corrective actions and management oversight.
37	A.5.37	Documented operating procedures	Applicable	Implemented	Documentation is available for selected technical activities (e.g. system usage, server-related tasks), formally approved operating procedures are in place.
A.7 People Controls					
38	A.6.1	Screening	Applicable	Implemented	The organization performs personnel screening prior to employment in accordance with applicable legal requirements and role criticality. Screening activities include verification of identity, references, integrity where applicable, and assessment of technical competencies relevant to the position. The scope of screening is proportionate to information security risks associated with the role.
39	A.6.2	Terms and conditions of employment	Applicable	Implemented	Employment contracts include information security obligations, confidentiality requirements, data protection responsibilities and consequences of non-compliance. Employees formally acknowledge their responsibilities related to information security and protection of organizational information assets.
40	A.6.3	Information security awareness, education and training	Applicable	Implemented	The organization provides regular information security awareness and training activities. Training includes onboarding sessions for new employees and recurring refresher training for existing staff. Awareness materials are maintained and aligned with internal policies, identified risks and security objectives.
41	A.6.4	Disciplinary process	Applicable	Implemented	A formal disciplinary process addressing violations of information security requirements is established. Disciplinary measures are defined within employment contracts and internal regulations and are applied consistently in accordance with labor legislation.
42	A.6.5	Responsibilities after termination or change of employment	Applicable	Implemented	Information security responsibilities following termination or change of employment are clearly defined. Access rights are revoked, organizational assets are returned, and confidentiality obligations remain applicable after the end of employment, as defined in contractual agreements.
43	A.6.6	Confidentiality or non-disclosure agreements	Applicable	Implemented	NDAs are included as part of employment and contractual documentation.
44	A.6.7	Remote working	Applicable	Implemented	Formal rules for remote working and home office arrangements are defined in internal policies. Remote access is protected through appropriate technical controls, including secure cloud services and multi-factor authentication.
45	A.6.8	Information security event reporting	Applicable	Implemented	Employees are informed and trained on how to identify and report information security events and incidents. Reporting procedures, escalation paths and responsibilities are defined in internal directives and supported through awareness activities.

#	ID	Control Name	Applicability	Implementation Status	Explanatory Notes
A.7 Physical Controls					
46	A.7.1	Physical security perimeters	Applicable	Implemented	Physical security perimeters are defined for office premises. Access to the building is controlled through secured entry points, including key-based access, security services (24/7 security staff), and turnstiles. Office areas are accessible only to authorized personnel, and access rights are managed and monitored.
47	A.7.2	Physical entry	Applicable	Implemented	Physical entry to the organization's premises is controlled through a combination of building access mechanisms, security personnel and restricted access to office areas. Access permissions are granted only to authorized employees and are reviewed as part of access management processes.
48	A.7.3	Securing offices, rooms and facilities	Applicable	Implemented	Office areas are secured outside working hours through building-level security services. Offices are accessible only to authorized personnel, and visitor access is controlled in accordance with internal rules.
49	A.7.4	Physical security monitoring	Applicable	Partially implemented	Physical security monitoring is provided at the building level through continuous security presence. Dedicated monitoring systems such as alarms or CCTV are not deployed within office premises, as no critical infrastructure or server rooms are located onsite and risks are mitigated through compensating controls.
50	A.7.5	Protecting against physical and environmental threats	Applicable	Partially implemented	The organization does not operate on-premises information processing facilities or server rooms. Environmental protection measures are therefore primarily ensured by cloud service providers. Office premises rely on building-level protections; no dedicated environmental monitoring systems are deployed internally due to limited risk exposure.
51	A.7.6	Working in secure areas	Applicable	Implemented	Rules for working in areas with increased sensitivity are defined and documented. The behavior of employees, visitors and external parties is governed by internal policies and communicated as part of awareness activities.
52	A.7.7	Clear desk and clear screen	Applicable	Implemented	Clear desk and clear screen rules are formally defined in internal policies. Employees are informed of these requirements through awareness activities and training.
53	A.7.8	Equipment siting and protection	Applicable	Implemented	Workstations and equipment are positioned to minimize the risk of unauthorized access, theft or damage. Visual exposure of sensitive information is limited, including appropriate positioning of screens.
54	A.7.9	Security of assets off-premises	Applicable	Partially implemented	Rules for the use of devices outside office premises are defined. A portion of endpoint devices is managed through mobile device management (MDM) using cloud-based solutions. Multi-factor authentication is enforced for all user accounts. Remaining unmanaged devices are subject to compensating controls and included in a phased onboarding plan.
55	A.7.10	Storage media	Applicable	Implemented	Rules governing the use of removable storage media, including USB devices and external drives, are defined. Usage is restricted and controlled in accordance with internal policies.
56	A.7.11	Supporting utilities	Applicable	Implemented	Supporting utilities such as power supply and internet connectivity are ensured through contractual arrangements with building management and service providers. As information processing is primarily cloud-based, availability risks related to local utilities are limited.
57	A.7.12	Cabling security	Not applicable	N/A	The organization does not operate significant on-premises cabling infrastructure supporting critical information systems. Information processing is cloud-based, and cabling-related risks are minimal. No dedicated cabling security procedures are defined due to limited applicability.
58	A.7.13	Equipment maintenance	Applicable	Implemented	Equipment maintenance is performed on a regular basis, either internally or through approved service providers. Maintenance activities are carried out with consideration for information security and data protection requirements.
59	A.7.14	Secure disposal or re-use of equipment	Applicable	Implemented	Procedures for secure disposal and reuse of equipment are defined. Data is securely erased prior to disposal or reassignment of devices, in accordance with internal policies.
A.8 Technological Controls					
60	A.8.1	User endpoint devices	Applicable	Partially implemented	Endpoint devices are partially managed using Microsoft Intune. Managed devices are subject to mobile device management (MDM) policies, security configurations and endpoint protection using Microsoft Defender. A subset of devices is not yet onboarded into Intune and is therefore not fully covered by centralized management and EDR controls. A phased onboarding plan is in place.
61	A.8.2	Privileged access rights	Applicable	Implemented	Privileged accounts are strictly limited, separated from standard user accounts and used only when required. Assignment and use of privileged access rights are controlled, approved and monitored in accordance with internal access management policies.
62	A.8.3	Information access restriction	Applicable	Implemented	Access to information systems and data is managed using role-based access control (RBAC). Access rights are granted based on business need, formally approved and regularly reviewed.
63	A.8.4	Access to source code	Not applicable	N/A	The organization does not develop or manage source code internally.
64	A.8.5	Secure authentication	Applicable	Implemented	Secure authentication mechanisms are enforced across the organization. Multi-factor authentication (MFA) is implemented for all user accounts, supported by centralized identity management using Microsoft Entra ID. Password policies enforce complexity and security requirements.
65	A.8.6	Capacity management	Applicable	Implemented	Capacity, performance and availability of cloud services are monitored continuously. Capacity management is primarily handled through cloud service provider capabilities and monitoring tools.
66	A.8.7	Protection against malware	Applicable	Partially implemented	Malware protection is implemented on managed endpoint devices using Microsoft Defender. Devices not yet onboarded into Intune are not fully covered by centralized endpoint protection. Risk is mitigated through account-level security controls and planned device onboarding.
67	A.8.8	Management of technical vulnerabilities	Applicable	Partially implemented	Patch management and vulnerability monitoring are implemented on managed devices through Intune and cloud-based security services. Devices not onboarded into centralized management are subject to compensating controls. Vulnerability remediation follows a risk-based approach.
68	A.8.9	Configuration management	Applicable	Implemented	Secure configuration baselines are defined and applied. Changes to system configurations are controlled through formal change management processes and aligned with security requirements.
69	A.8.10	Information deletion	Applicable	Implemented	Rules and procedures for secure deletion of information are defined and implemented. Data deletion complies with retention requirements, GDPR and internal data management policies.
70	A.8.11	Data masking	Applicable	Implemented	Data masking and anonymization techniques are applied, particularly in test and non-production environments, to protect sensitive and personal data.
71	A.8.12	Data leakage prevention	Applicable	Partially implemented	Data leakage prevention (DLP) controls are implemented within Microsoft 365. Controls include monitoring, sharing restrictions and enforcement of data protection rules.
72	A.8.13	Information backup	Applicable	Implemented	Information is backed up regularly, with backups performed daily. Backup restoration is tested periodically. Backup requirements and responsibilities are defined in a dedicated internal policy.
73	A.8.14	Redundancy of information processing facilities	Applicable	Implemented	Availability and redundancy are ensured through cloud service provider infrastructure and contractual service level agreements (SLAs).
74	A.8.15	Logging	Applicable	Partially implemented	Security and system logs are generated and monitored for managed devices and cloud services. Logging coverage for endpoint devices is dependent on Intune onboarding status. Centralized logging is applied where technically supported.
75	A.8.16	Monitoring activities	Applicable	Implemented	Security monitoring and alerting mechanisms are in place. Detected events are assessed and handled in accordance with incident management procedures.
76	A.8.17	Clock synchronization	Applicable	Implemented	Time synchronization relies on default operating system and Microsoft cloud settings.
77	A.8.18	Use of privileged utility programs	Applicable	Implemented	Use of privileged utilities and administrative tools is restricted, authorized and logged. Access is granted only to users with defined administrative responsibilities.
78	A.8.19	Installation of software on operational systems	Applicable	Partially implemented	Software installation is controlled and approved on managed devices. Enforcement of installation restrictions depends on device onboarding into centralized management systems.
79	A.8.20	Networks security	Applicable	Implemented	The organization operates a cloud-based architecture without an internal on-premises network. Network security is ensured through cloud service provider controls, secure authentication and access restrictions.
80	A.8.21	Security of network services	Applicable	Implemented	Network services are secured, monitored and covered by contractual agreements with cloud and connectivity service providers.
81	A.8.22	Segregation of networks	Applicable	Implemented	Production and test environments are logically and physically separated. Access controls and environment segregation are formally defined and enforced.
82	A.8.23	Web filtering	Applicable	Partially implemented	Web filtering and protection against malicious websites are not yet fully implemented. Compensating controls are applied at account and service level. Implementation of URL filtering is planned.
83	A.8.24	Use of cryptography	Applicable	Implemented	Cryptographic controls are used to protect data at rest and in transit. Encryption mechanisms are provided by cloud platforms and applied in accordance with security requirements.
84	A.8.25	Secure development life cycle	Applicable	Implemented	Security requirements are defined for the software development lifecycle and enforced through contractual and procedural controls with external development providers.
85	A.8.26	Application security requirements	Applicable	Implemented	Application security requirements are formally defined and communicated to development and service providers.
86	A.8.27	Secure system architecture and engineering principles	Applicable	Implemented	Secure architecture and engineering principles are defined and applied when designing and operating information systems and services.
87	A.8.28	Secure coding	Applicable	Implemented	Secure coding requirements are formally defined and enforced through internal policies and contractual obligations with external developers.
88	A.8.29	Security testing in development and acceptance	Applicable	Implemented	Security testing of applications (including penetration testing) is performed as part of development and acceptance processes. Testing requirements are documented and applied consistently.
89	A.8.30	Outsourced development	Applicable	Implemented	Software development is outsourced. Security requirements, responsibilities and controls are defined contractually and monitored.
90	A.8.31	Separation of development, test and production environments	Applicable	Implemented	Development, test and production environments are formally separated. Promotion of changes follows defined approval and testing procedures.
91	A.8.32	Change management	Applicable	Implemented	Changes to information systems are documented, reviewed and approved through a formal change management process.
92	A.8.33	Test information	Applicable	Implemented	Test data are protected and anonymized. Test environments are separated from production systems.
93	A.8.34	Protection of information systems during audit testing	Applicable	Implemented	Rules and procedures are defined to ensure protection of information systems during audit and security testing activities.