ANNEX A	APPLICABLE?
ISO 27001 5.1 Policies for information security	YES
ISO 27001 5.2 Information security roles and responsibilities	YES
ISO 27001 5.3 Segregation of duties	YES
ISO 27001 5.4 Management responsibilities	YES
ISO 27001 5.5 Contact with authorities	YES
ISO 27001 5.6 Contact with special interest groups	YES
ISO 27001 5.7 Threat intelligence – new	YES
ISO 27001 5.8 Information security in project management	YES
ISO 27001 5.9 Inventory of information and other associated assets – change	YES
ISO 27001 5.10 Acceptable use of information and other associated assets – change	YES
ISO 27001 5.11 Return of assets	YES
ISO 27001 5.12 Classification of information	YES
ISO 27001 5.13 Labelling of information	YES
ISO 27001 5.14 Information transfer	YES
ISO 27001 5.15 Access control	YES
ISO 27001 5.16 Identity management	YES
ISO 27001 5.17 Authentication information – new	YES
ISO 27001 5.18 Access rights – change	YES
ISO 27001 5.19 Information security in supplier relationships	YES
ISO 27001 5.20 Addressing information security within supplier agreements	YES
ISO 27001 5.21 Managing information security in the ICT supply chain – new	YES
ISO 27001 5.22 Monitoring, review and change management of supplier services – change	YES
ISO 27001 5.23 Information security for use of cloud services – new	YES
ISO 27001 5.24 Information security incident management planning and preparation – change	YES
ISO 27001 5.25 Assessment and decision on information security events	YES
ISO 27001 5.26 Response to information security incidents	YES
ISO 27001 5.27 Learning from information security incidents	YES
ISO 27001 5.28 Collection of evidence	YES
ISO 27001 5.29 Information security during disruption – change	YES
ISO 27001 5.30 ICT readiness for business continuity – new	YES
ISO 27001 5.31 Identification of legal, statutory, regulatory and contractual requirements	YES
ISO 27001 5.32 Intellectual property rights	YES
ISO 27001 5.33 Protection of records	YES
ISO 27001 5.34 Privacy and protection of PII	YES
ISO 27001 5.35 Independent review of information security	YES
ISO 27001 5.36 Compliance with policies and standards for information security	YES
ISO 27001 5.37 Documented operating procedures	YES
ISO 27001 6 People controls	
ISO 27001 6.1 Screening	YES
ISO 27001 6.2 Terms and conditions of employment	YES
ISO 27001 6.3 Information security awareness, education and training	YES
ISO 27001 6.4 Disciplinary process	YES
ISO 27001 6.5 Responsibilities after termination or change of employment	YES
ISO 27001 6.6 Confidentiality or non-disclosure agreements	YES
ISO 27001 6.7 Remote working – new	YES
ISO 27001 6.8 Information security event reporting	YES
ISO 27001 7 Physical controls	
ISO 27001 7.1 Physical security perimeter	NO
ISO 27001 7.2 Physical entry controls	NO
ISO 27001 7.3 Securing offices, rooms and facilities	NO
ISO 27001 7.4 Physical security monitoring	NO
ISO 27001 7.5 Protecting against physical and environmental threats	NO
ISO 27001 7.6 Working in secure areas	NO
ISO 27001 7.7 Clear desk and clear screen	YES
ISO 27001 7.8 Equipment siting and protection	NO
ISO 27001 7.9 Security of assets off-premises	YES

ISO 27001 7.10 Storage media – new	YES
ISO 27001 7.11 Supporting utilities	NO
ISO 27001 7.12 Cabling security	NO
ISO 27001 7.13 Equipment maintenance	NO
ISO 27001 7.14 Secure disposal or re-use of equipment	NO

ISO 27001 8 Technological controls

ISO 27001 8.1 User endpoint devices – new	YES
ISO 27001 8.2 Privileged access rights	YES
ISO 27001 8.3 Information access restriction	YES
ISO 27001 8.4 Access to source code	NO
ISO 27001 8.5 Secure authentication	YES
ISO 27001 8.6 Capacity management	YES
ISO 27001 8.7 Protection against malware	YES
ISO 27001 8.8 Management of technical vulnerabilities	NO
ISO 27001 8.9 Configuration management	NO
ISO 27001 8.10 Information deletion – new	YES
ISO 27001 8.11 Data masking – new	YES
ISO 27001 8.12 Data leakage prevention – new	YES
ISO 27001 8.13 Information backup	YES
ISO 27001 8.14 Redundancy of information processing facilities	NO
ISO 27001 8.15 Logging	NO
ISO 27001 8.16 Monitoring activities	YES
ISO 27001 8.17 Clock synchronization	NO
ISO 27001 8.18 Use of privileged utility programs	NO
ISO 27001 8.19 Installation of software on operational systems	NO
ISO 27001 8.20 Network controls	NO
ISO 27001 8.21 Security of network services	NO
ISO 27001 8.22 Web filtering – new	NO
ISO 27001 8.23 Segregation in networks	NO
ISO 27001 8.24 Use of cryptography	NO
ISO 27001 8.25 Secure development lifecycle	NO
ISO 27001 8.26 Application security requirements – new	NO
ISO 27001 8.27 Secure system architecture and engineering principles – new	NO
ISO 27001 8.29 Security testing in development and acceptance	NO
ISO 27001 8.30 Outsourced development	NO
ISO 27001 8.31 Separation of development, test and production environments	NO
ISO 27001 8.32 Change management	YES
ISO 27001 8.33 Test information	NO
ISO 27001 8.34 Protection of information systems during audit and testing – new	NO

20231213 - ISO27001 Statement Of Applicability GH