Memset Statement of Applicability

Owner

Head of Compliance

Purpose

To protect information and assets owned by or entrusted to Memset by means of mapping out the measures and controls in place, which provide a framework and established processes which meet the requirements set out in the ISO 27001:2013 Standard.

Affected Parties

All Memset Employees.

Definitions

ISMS: Information Security Management System

Review and Maintenance:

At a minimum, this document shall be reviewed annually or if a significant change to the Memset ISMS occurs

The following Statement of Applicability summarises the objectives and controls that are relevant and applicable to the Memset Information Security Management System (ISMS) in accordance with the requirements of ISO 27001:2013 (Information Security).

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.5.1.1	Yes	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.			x		Memset Security Policy
A.5.1.2	Yes	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.			x		Memset Security Policy / Quarterly ISMS Management review
A6. Organisation of information security							
A.6.1 Internal organisation							
A.6.1.1	Yes	All information security responsibilities shall be defined and allocated.			x		Compliance Manual / HR system role definitions
A.6.1.2	Yes	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.			x		Compliance Manual
A.6.1.3	Yes	Appropriate contacts with relevant authorities shall be maintained.	x				Compliance Manual / Process for contact with law enforcement and PSNA
A6.1.4	Yes	Appropriate contacts with special interest groups or other specialist Security forums and professional associations shall be maintained.			x		Compliance Manual / Tech UK, 10% group, CISP, Trusted Access Forum, Xen vulnerability pre-disclosure group
A.6.1.5	Yes	Information security shall be addressed in project management, regardless of the type of the project.			x		Compliance Manual
A.6.2 Mobile Devices and Teleworking							
A.6.2.1	Yes	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.			x		No use of mobile devices for Memset email/credentials. Office wireless network segregated.
A.6.2.2.	Yes	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites			x		IT Usage Policy defines device security, internal VPN system to access highly sensitive systems e.g. file stores
A.7 Human resource security							
A.7.1 Prior to employment							
A.7.1.1	Yes	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the	x	x	x		HR New Starter Process / Employee Terms and Conditions BPSS checks for all staff prior to employment. SC for staff who access the PSN estate.

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
		classification of the information to be accessed and the perceived risks.					
A.7.1.2	Yes	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	x				HR New Starter Process / Employee Terms and Conditions / Security IT Usage policy
A.7.2 During employment							
A.7.2.1	Yes	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.			x		Compliance Manual / Information Classification Policy / HR New starter process / AUP policy / Security Training and Awareness Process
A.7.2.2	Yes	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.			x		Compliance Manual / Information Classification Policy / HR New starter process / AUP policy / Security Training and Awareness Process
A.7.2.3	Yes	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed and formation security breach.	x		x		Disciplinary Policy / Employee terms and conditions
A.7.3 Termination and change of employment							
A.7.3.1	Yes	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.		x	x		HR Leavers policy / Access Management Policy All terminated employees assets are always retrieved, unless transferred to the employee under the employee asset transfer agreement. Part of this agreement is that the corporate infrastructure team will format before the asset is handed over.
A.8 Asset Management							
A.8.1 Responsibility for assets							
A 8.1.1	Yes	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.			x		Asset Management system
A.8.1.2	Yes	Assets maintained in the inventory shall be owned.			x		Compliance Manual and Asset Management System
A.8.1.3	Yes	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.			x		Corporate IT standard.
A.8.1.4	Yes	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.			x		Asset Management / Leavers Process
A.8.2 Information classification							

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.8.2.1	Yes	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.			x		Information Classification Policy
A.8.2.2	Yes	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.			x		Information Classification Policy
A.8.2.3	Yes	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.			x		Information Classification Policy Asset Management / Leavers Process
A.8.3 Media Handling							
A.8.3.1	Yes	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.		x	x		Corporate IT Standard
A.8.3.2	Yes	Media shall be disposed of securely when no longer required, using formal procedures.		x	x		Corporate IT Standard / All media given back to Corporate Infrastructure for destruction. / Customer data destruction as per
A.8.3.3	Yes	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.		x	x		Access Management policy / HR change of employment policy.
A.9 Access control							
A.9.1 Business requirements of access control							
A.9.1.1	Yes	An access control policy shall be established, documented and reviewed based on business and information security requirements.			x		Secure Working Environment / Corporate IT Standard /Access policy
A.9.1.2	Yes	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.			x		Secure Working Environment / Corporate IT Standard /Access policy
A.9.2 User access management							
A.9.2.1	Yes	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.			x		Secure Working Environment / Corporate IT Standard /Access policy
A.9.2.2	Yes	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.			x		Secure Working Environment / Corporate IT Standard /Access policy
A.9.2.3	Yes	The allocation and use of privileged access rights shall be restricted and controlled.			x		Secure Working Environment / Corporate IT Standard /Access policy
A.9.2.4	Yes	The allocation of secret authentication information shall be controlled through a formal management process.			x		Secure Working Environment / Corporate IT Standard
A.9.2.5	Yes	Asset owners shall review users' access rights at regular intervals.			x		Corporate IT Standard / Reviews

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.9.2.6	Yes	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.			x		Corporate IT Standard
A.9.3 User responsibilities							
A.9.3.1	Yes	Users shall be required to follow the organization's practices in the use of secret authentication information.			x		IT usage policy / Password Policy
A9.4 System and application access control							
A.9.4.1	YEs	Access to information and application system functions shall be restricted in accordance with the access control policy.		x	x		Physical and logical restrictions
A.9.4.2	Yes	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.			x		2 centralised authentication planes w HT access keys (strong apache layer auth), SSH keys for privileged access, domain authentication using LDAP under test on CCTV, physical access management & PSN systems
A.9.4.3	Yes	Password management systems shall be interactive and shall ensure quality passwords.			x		Password generator, strong password policy, KeePass encrypted storage.
A.9.4.4	Yes	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.			x		Personal devices: policies, tech assistance from Biz Services, personnel vetting. Internal systems: SSH key access control, role based, segregation of customer & internal infrastructure, OSSEC & system logging & alerting
A.9.4.5	Yes	Access to program source code shall be restricted.			x		Django permission, changelog, process for submitting changes
A.10 Cryptography							
A.10.1 Cryptographic controls							
A.10.1.1	Yes	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.			x		Cryptographic Controls Policy
A.10.1.2	Yes	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.			x		Cryptographic Controls Policy
A.11 Physical and environmental security							
A.11.1 Secure areas							
A.11.1.1	Yes	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.		x	x		Perimeter fence, datacentre perimeter, office perimeter/ Access Management Policy / Information Classification Policy
A.11.1.2	Yes	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.			x		Secure Working Environment Policy / Physical security controls, 2 factor authentication for access. CCTV. Visitor controls

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.11.1.3	Yes	Physical security for offices, rooms and facilities shall be designed and applied.			x		Secure Working Environment Policy / Physical security controls, 2 factor authentication for access. CCTV. Visitor controls
A.11.1.4	Yes	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	x		x		Low risk flood area. Fire RA and controls implemented. Physical security Inc. crash barriers
A.11.1.5	Yes	Procedures for working in secure areas shall be designed and applied.			x		Secure Working Environment Policy / Physical security controls, 2 factor authentication for access. CCTV. Visitor controls
A.11.1.6	Yes	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.			x		Secure Working Environment Policy / Physical security controls, 2 factor authentication for access. CCTV. Visitor controls Air lock in DC. Reception area for the office. Asset managing.
A 11.2 Equipment							
A.11.2.1	Yes	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		x	x		Generators' fencing. All other equipment inside datacentre and office perimeters.
A.11.2.2	Yes	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.			x		UPS's protect key equipment until generators come online
A.11.2.3	Yes	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.			x		All underground. Terminate within perimeter.
A.11.2.4	Yes	Equipment shall be correctly maintained to ensure its continued availability and integrity.	x		x		Schedule in place (DC maintenance schedule)
A.11.2.5	Yes	Equipment, information or software shall not be taken off-site without prior authorization.			x		IT Usage Policy, BAU activities allowed, outside of that line manager permission required.
A.11.2.6	Yes	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.			x		Security evaluations of co-lo providers
A.11.2.7	Yes	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.		x	x		Data Destruction Policy and Leaving Procedure
A.11.2.8	Yes	Users shall ensure that unattended equipment has appropriate protection.			x		Must use automatic password protected screensaver - IT Usage Policy
A.11.2.9	Yes	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.			x		Password protected screen saver mandatory (IT Usage Policy), clear desk policy in Security Manual.
A.12 Operations Security							
A.12.1 Operational procedures and responsibilities							

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.12.1.1	Yes	Operating procedures shall be documented and made available to all users who need them.			x		Compliance Manual / Corporate Wiki
A.12.1.2	Yes	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.			x		Risk Assessment process / Audits (internal and external) / Management reviews / Change process
A.12.1.3	Yes	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.			x		HR Capacity Management / Management Reviews / Ops Meetings / Monitoring systems re. disk usage, RAM etc. / provisioning systems monitor purchasing levels
A.12.1.4	Yes	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.			x		Change Management Process
A12.2 Protection from Malware							
A 12.2.1	Yes	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness			x		Requirement for AV where applicable, user awareness through induction & ongoing alerts, audits, IT usage policy, backups to recover from attacks, Security Manager monitors vulnerability alerts
A.12.3 Backup							
A.12.3.1	Yes	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.		x	x		Memset Backup Data Policy
A.12.4 Logging and monitoring							
A.12.4.1	Yes	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.		x	x		Activities, faults & info sec events logged. Faults trigger bang message to dev for resolution. Info sec events > security manager and incident management procedure. Activities reviewed when event necessitates it.
A.12.4.2	Yes	Logging facilities and log information shall be protected against tampering and unauthorized access.			x		Logs retained for minimum 1 yr. immutable. ADD
A.12.4.3	Yes	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.			x		Nagios monitors network activity. Managed by Biz Services not Ops. Activities logged and protected as above.
A.12.4.4	Yes	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.			x		Laptops all internet connected. NTP servers used.
A.12.5 Control of operational software							
A.12.5.1	Yes	Procedures shall be implemented to control the installation of software on operational systems.			x		Trained SysAds, documented procedures, verified GPG signed packages & MD5 checksums, multiple testing environments w workflow, all config tracked in SVN, some security updates automatic others require prior testing, local server logging, trac tickets for managing changes, laptop

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
							management by Biz Services
A.12.6 Technical Vulnerability Management							
A.12.6.1	Yes	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.		x	x		Technical management receive vulnerability alerts and assess and act accordingly, pre-release notifications
A.12.6.2	Yes	Rules governing the installation of software by users shall be established and implemented.			x		Users have admin rights to personal devices but supported by IT Usage Policy (installation from untrusted site prohibited, software updates), training and advice from Security Manager. Devices audited.
A.12.7 Information systems audit considerations							
A.12.7.1	Yes	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.			x		Internal audit and Corrective Action programme and schedule in place and ensure minimal disruption.
A.13 Communications security							
A.13.1 Network security management							
A.13.1.1	Yes	Networks shall be managed and controlled to protect information in systems and applications.			x		Segregation of duties - Network Manager, Ops Manager & Biz Services Manager, centralised logging, monitoring system alerts for disruptive activity, management meetings and security forums for co-ordination
A.13.1.2	Yes	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.			x		Network service primarily designed & managed in house, standard contracts & SLAs w BT, Everest, HE & LINX, access to significant systems over encrypted channels e.g. HTTPS & SSH, segregated networks
A.13.1.3	Yes	Groups of information services, users and information systems shall be segregated on networks.			x		vLANs for internal and customer segregation, restricted WiFi permissions, transient logging, physically segregated PSN network, geographically network paths & network equipment
A.13.2.1	Yes	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.			x		Procedure for disclosing classified information, GPG for sensitive info, IT usage policy, security of mail server and IM server, grey listing & virus checking on email gateway
A.13.2.2	Yes	Agreements shall address the secure transfer of business information between the organization and external parties.			x		Disclosing Classified Info Procedure, Media in Transit Policy
A.13.2.3	Yes	Information involved in electronic messaging shall be appropriately tested.			x		Email & IM. Hardened, closely monitored infrastructure,
A.13.2.4	Yes	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information	x	x	x		Customer T&C's, NDA's and Employee confidentiality terms in place

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
		shall be identified, regularly reviewed and documented.					
A.14 System acquisition, development and maintenance.							
A.14.1 Security requirements of information systems.							
A.14.1.1	Yes	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.			x		Incidents, risk assessments, vulnerabilities & regulation inform security requirements. Discussion at board and management level. Corporate Infrastructure Services managed by Security Manager. Consideration in recruitment.
A.14.1.2	Yes	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.			x		VPN access for filestores & customer support w SSH key or username/password. Web accessible apps: HT access keys, hardened cypher suite and servers
A.14.1.3	Yes	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.			x		API endpoints: hardened servers, hardened cypher suites, restricted access, TLS. API keys: 32 bit hex random strings, rate limiting, monitor brute force attacks, optional white listing. Customers: can restrict granular access
A.14.2 Security in development and support processes							
A.14.2.1	Yes	Rules for the development of software and systems shall be established and applied to developments within the organization.		x	x		Dev Release Procedure, dev environment secured, multiple layers of testing, secure repositories, version control, rigorous recruitment procedure, culture of asking team for assistance & advice
A.14.2.2	Yes	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.			x		Dev release procedure, Buildbot tests, alerts to dev team when code submitted to Buildbot, SVN access controlled, manual Q&A testing prior to going live, SVN logs all changes with full details, version control
A.14.2.3	Yes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.			x		Email alerts when code passes Buildbot, code review in dev environment, beta release when necessary
A.14.2.4	Yes	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.			x		Modification rare submit bug reports instead, requires management authorisation, if occurs change merged back asap
A.14.2.5	Yes	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.			x		Django enforces Model View Code principles
A.14.2.6	Yes	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.			x		Laptops encrypted, SVN accessed over SSH, dev environment accessed over SSH, logging, access control
A.14.2.7	Yes	The organization shall supervise and monitor the activity of outsourced system development.			x		Very rare, no access to Memset code or systems, access restricted to separate repository
A.14.2.8	Yes	Testing of security functionality shall be carried out during development.			x		Annual external pen tests, internal Buildbot tests (unit, regression, static pylint checking) & manual code reviews

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.14.2.9	Yes	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.			x		Internal Buildbot tests, external programs tested in dev environment prior to use
A.14.3 Test data							
A.14.3.1	Yes	Test data shall be selected carefully, protected and controlled.			x		Test data from database is automatically anonymised after a snapshot of a live system is taken. Names, emails etc. replaced, no data off customer servers ever used.
A.15 Supplier relationships							
A.15.1 Information security in supplier relationships							
A.15.1.1	Yes	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.			x		Very little supplier access, agreement in place with Everest, LINX & HE and regular security audits
A.15.1.2	Yes	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.		x	x		Few security impacting suppliers, appropriate agreements in place
A.15.1.3	Yes	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.			x		Where applicable these are in place e.g. penetration testers
A.15.2 Supplier service delivery management							
A.15.2.1	Yes	Organizations shall regularly monitor, review and audit supplier service delivery.		x	x		Supplier Evaluation Procedure combined with the schedule
A.15.2.2	Yes	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.		x	x		Managed by the Memset supplier contact, usually Technical Buyer, sometimes applicable manager e.g. Network Manager manages relationship with fibre providers
A.16 Information security incident management							
A.16.1 Management of information security incidents and improvements							
A.16.1.1	Yes	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.					Compliance Manual / Incident Management policy and process
A.16.1.2	Yes	Information security events shall be reported through appropriate management channels as quickly as possible.	x	x	x		Compliance Manual / Incident Management policy and process

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.16.1.3	Yes	Employees and contractors using the organization's information systems and services shall be required to note and report an observed or suspected information security weaknesses in systems or services.	x	x	x		Incident Management policy and process
A.16.1.4	Yes	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.			x		Incident Management policy and process / Internal audit programme
A.16.1.5	Yes	Information security incidents shall be responded to in accordance with the documented procedures.			x		Incident Management policy and process / Risk Management policy and process
A.16.1.6	Yes	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.			x		Incident Management policy and process / Risk Management policy and process
A.16.1.7	Yes	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.			x		Incident Management policy and process / Risk Management policy and process
A.17 Information security aspects of business continuity management							
A.17.1 Information security continuity							
A.17.1.1	Yes	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.			x		Business Continuity Policy
A.17.1.2	Yes	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.			x		Business Continuity Policy
A.17.1.3	Yes	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.			x		Business Continuity Policy
A.17.2 Redundancies							
A.17.2.1	Yes	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.			x		Business Continuity Policy
A.18 Compliance							
A.18.1 Compliance with legal and contractual requirements							
A.18.1.1	Yes	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.			x		Compliance with Legal standards Policy / Security Policy

Control Ref:.	Applicable	Control	Reason code*				Comment / Location of Supporting Information
			L	C	B	R	
A.18.1.2	Yes	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary soft-ware products.			x		Compliance with Legal standards Policy / Security Policy / Internal Audit programme
A.18.1.3	Yes	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislation, regulatory, contractual and business requirements.			x		Information Classification Policy / Document and Record control Policy / Key docs in wiki. Multiple filestores with varying access. Granular access permissions.
A.18.1.4	Yes	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.			x		Information Classification Policy / Document and Record control Policy
A.18.1.5	Yes	Cryptographic controls shall be used in compliance with all relevant requirements, legislation and regulations.	x	x	x		We don't import/export computer hardware or software which performs cryptographic capabilities. Have engaged with GCHQ re use of encryption. Law enforcement contact procedure in place.
A.18.2 Information security reviews							
A.18.2.1	Yes	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, pro-cesses and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.		x	x		Bi Annual External Audit
A.18.2.2	Yes	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.			x		ISMS Management review / Weekly operations review, compliance update
A.18.2.3	Yes	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.			x		Internal audit programme

*Reason codes listed as follows:

L = Legal or regulatory requirement

C = Contractual obligation/s

B = Business requirement or adopted best practice

R = Result of a risk assessment

Note: Risk management procedure and associated treatment plans underpin the entire system and are not necessarily noted individually above.

Reference

Compliance Manual

Change & Review Record

Version	Date	Detail of Change or Review
5	30.06.2016	Re formatted and revised document. Created in line with new policy and process templates.