Estate Insurance Group			V1	Issue Date: 8.10.14
Information Security - Controls				
Annex A reference	**Control description**		**Implemented Controls / Applicability Associated Documents**	**Comments**
A.6.2 Mobile devices and teleworking				
Objective: To ensure the security of teleworking and use of mobile devices.				
A.6.2.1	Mobile device policy	*Control* A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	The company has issued a Mobile device policy	
A.7.3 Termination and change of employment				
Objective: To protect the organization's interests as part of the process of changing or terminating employment				
A.7.3.1	Termination or change of employment responsibilities	*Control* 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.	The Managing Director will oversee any termination requirements, to ensure that correct procedures are adopted. The Director will consult the Co's employment advisor on complex HR related issues.	
A.8.3 Media handling				
Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.				
A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	The Company details its arrangements for the handling of removable media as detailed within the 'Information Classification' guidelines. Procedures are also denoted within data security presentations issued to employees	
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.	The Company has developed formal procedures for disposal of media.	
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.	The Company sets out agreed procedures for protecting against: access, misuse or corruption of data (the asset) during transportation within the 'Information Classification' sheet	
A.9 Access control				
A.9.1 Business requirements of access control				
Objective: To limit access to information and information processing facilities.				
A.9.1.2	Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorised to use.	Network devices (firewalls, routers and switches) are configured according to manufacturers guidelines. Default device passwords are changed.	
A.9.2 User access management				
Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.				
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.	The MD & IT Contractor will review access rights at the Company's scheduled Security forum meetings or after any changes, such as change of employment status.	
A.9.2.6	Removal or adjustment of access rights	*Control* 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.	The MD will remove all access rights immediately upon a member of staff leaving or as advised by the Managing Director.	
A.9.4 System and application access control				

Objective: To prevent unauthorised access to systems and applications.				
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Secure 'log-on' procedures are controlled by the Operating System (OS) and/or the 'cloud' service application(s). The company has determined the maximum time for an 'inactive session' is 10 minutes before 'lockout' occurs. This reflects the security risks to the company, the classification of the information and the applications being used. After a maximum of three (5) consecutive login failures the account is locked out for 15 minutes.	
A.9.4.3	Password management system	*Control* Password management systems shall be interactive and shall ensure quality passwords.	Active Directory Policy Ensures Password Complexity	
A.11 Physical and environmental security				
A.11.1 Secure areas				
Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.				
A.11.1.1	Physical security perimeter	*Control* Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Brick Built Building with Locked Doors and Windows	
A.11.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Appropriate perimeters are defined for secure areas and access to secure areas are restricted to authorised staff only.	
A.11.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms and facilities shall be designed and applied.	Critical areas such as server location are securely locked and located to ensure minimum disruption can take place. A mechanical lock is used and only authorised staff have access to the server room at appropriate times.	
A.11.1.4	Protecting against external and environmental threats	*Control* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	The organisation's risk (site and local) assessment takes into consideration potential threats from food, fire and disaster. Smoke detectors are installed in appropriate areas and the fire system is serviced on a regularly basis (check timescales). Fire extinguishers are appropriately positioned and serviced by a 3rd party contractor on a 12 monthly basis.	
A.11.1.6	Delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.	There is one access point for deliveries. Visitors/contractors are met by a staff member. Incoming items are registered in accordance with asset management procedures and stored accordingly.	
A.11.2 Equipment				
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.				
A.11.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.	Maintenance Agreements	
A.11.2.6	Security of equipment and assets off-premises	*Control* Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Mobile Device Security Policy	

A.11.2.7	Secure disposal or re-use of equipment	*Control* 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.	A log is maintained of all equipment requiring disposal. Any faulty hard drives are destroyed by an external contractor and certification issued.	
A.11.2.8	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.	Workstations & laptops are set to 'lock' after ten minutes of non use.	
A.12.2 Protection from malware				
Objective: To ensure that information and information processing facilities are protected against malware.				
A.12.2.1	Controls against malware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	The IT contractor ensures installation and regular updates of AV protection software to scan (full scan is scheduled weekly) computers and media on a routine basis. Staff are made aware that information systems are for business purposes, this is communicated in the the employee handbook.	
A.12.3 Backup				
Objective: To protect against loss of data.				
A.12.3.1	Information backup	*Control* Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Full tape backup(s) are performed: Mon-Fri. Scheduled remote backups take place nighty. Tapes are kept in a fire proof safe and removed offsite on a monthly basis. Backup tests are carried out monthly?	
A.12.6 Technical vulnerability management				
Objective: To prevent exploitation of technical vulnerabilities.				
A.12.6.1	Management of technical vulnerabilities	*Control* 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.	Reports from Pen Test	To be conducted.
A.12.6.2	Restrictions on software installation	*Control* Rules governing the installation of software by users shall be established and implemented.	Policy on Acceptable use of Assets Access Rights Register	
A.13.2 Information transfer				
Objective: To maintain the security of information transferred within an organization and with any external entity.				
A.13.2.2	Agreements on information transfer	*Control* Agreements shall address the secure transfer of business information between the organization and external parties.	Information Control Policy and Supplier Contracts	

A.13.2.3	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.	1-Refer to Email section in AUP Policy 2-The organisation uses the latest antivirus software to scan outbound/inbound email. 3-Disclaimers are attached to emails. 4-Staff are allowed limited use of personal email, this is documented in the AUP policy. 5-Email disclaimers have been prepared. Potential Legal threat areas covered by the disclaimer are: Breach of confidentiality, accidental breach of confidentiality, transmission of viruses, employer's liability.	
A.13.2.4	Confidentiality or non-disclosure agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	The Company will identify all confidentiality agreements required, together with non-disclosure agreements. Where identified appropriate documents will be prepared, issued and authorised and retained on file for inspection	
A.15 Supplier relationships				
A.15.1 Information security in supplier relationships				
Objective: To ensure protection of the organization's assets that is accessible by suppliers.				
A.15.1.1	Information security policy for supplier relationships	*Control* 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.	Supplier agreements clearly define measures for reducing/mitigating information security 'risks'. A policy is communicated to suppliers. Security Policy for Contractors	
A.15.1.2	Addressing security within supplier agreements	*Control* 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.	NDAs Confidentiality Agreements SLA's	
A.15.1.3	Information and communication technology supply chain	*Control* Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	The Company will maintain a listing of all key suppliers having access to or transferring 'assets'. Each contract will highlight the salient information security requirement. This must be approved & accepted by the supplier.	
A.16 Information security incident management				
A.16.1 Management of information security incidents and improvements				
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.				
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.	All contractors, visitors and employees are made aware of the Information Security Policy. Visitors must sign the Vistors Book on arrival. Staff nor visitors should use mobile phones within the working areas.	
A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	The MD Shall assess and classify information security incidents. This exercise will be logged within the Master NC spread-sheet.	

A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.	The Company has a procedure for handling non-compliance & security incidents. This is a controlled document.	
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the	The Master NC log details outcomes and opportunities for learning.	
A.18 Compliance				
A.18.1 Compliance with legal and contractual requirements				
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.				
A.18.1.1	Identification of applicable legislation and contractual requirements	*Control* 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.	The MD has created a controlled document that addresses key legislation pertaining to the industry. This listing is kept up to date & is verified annually.	
A.18.1.3	Protection of records	*Control* Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory,	Centralised servers contain corporate data. Access control and backup procedures provide appropriate protection.	
A.18.1.4	Privacy and protection of personally identifiable information	*Control* Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	The company has a Data Protection Policy. All staff receive data protection training delivered by the MD or nominee, which is reviewed and refreshed with all staff annually.	

Form Number: 59

Approved by : J S