Ross Packard – 01/05/2018

GDPR Information Security Policies

CONTENTS

Ross Packard GDPR Information Security Policies

This document contains Ross Packard's policies relating to information security.

01. Registration with the Information Commissioners Office

Ross Packard is registered with the Information Commissioner's Office and renews annually. The ICO outlines best practice regarding the reasons or purposes for processing information, the type of personal data processed, who it's about and who its shared with to enable Ross Packard to perform its services, maintain accounts and to manage staff within the law.

02. Cyber Security Accreditation

Cyber Essentials helps Ross Packard guard against the most common cyber threats and demonstrates our commitment to cyber security. We are Cyber Essentials certified and this certification reassures our customers we are working to secure our Internet connection, devices and software, controlling access to our data services, protecting our systems from viruses and other malware, and keeping our devices and software up to date. We are able to show we have cyber security measures in place and have a clear picture of our organisation's cyber security level.

03. Data Protection Act 1998 (Valid until 25th May 2018)

Ross Packard understands and abides by the provisions of the Data Protection Act 1998, designed to protect personal data stored on computers and organised filing systems, and which provides protection to the processing and movement of data. Staff are aware of the eight data protection principles of: 1. Processing personal data fairly and lawfully, 2. Only obtained for specified lawful purposes and not further processed, 3. Adequate, relevant and not excessive in relation to the purpose, 4. Accurate and up to date, 5. Not kept any longer than necessary, 6. Processed in accordance with the rights of individuals as data subjects, 7. Measures taken against unlawful processing, accidental loss, destruction or damage, and 8. Not transferred outside the EEA. (Please note that this is current legislation which expires 25 May 2018)

04. The General Data Protection Regulation 2016 (Enforced 25th May 2018)

The GDPR applies to any organisation who processes the Personally Data of individuals located within the EU. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of the controller. In cases where we act on behalf of a work provider, such as a motor insurer or network management company, we are a processor. Where we undertake work directly with individual customers, we are the controller. When we are a processor, we understand our legal obligations regarding the maintenance of personal data and processing activities, including our legal liability if responsible for a breach. (Please note that this becomes enforceable 25 May 2018 when the DPA expires)

05. Information Security Policy Statement

This policy has been approved by Ross Packard and any amendments require approval by Ross Packard. The policy provides the information required to enable you to ensure your area of business complies with the Policy. Support and guidance is offered by managers and a toolkit, which includes training, template policies, example risk assessments and guidance is available. Information Security is not a new requirement, and to a large extent this policy formalizes and regulates existing good practice. This policy provides a framework for the management of information security throughout Ross Packard.

It applies to all those with access to Packard information systems, including staff, visitors and contractors, any system attached to Ross Packard computer or telephone networks and any systems supplied to Ross Packard. Also, all information (data) processed by Ross Packard pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from Ross Packard and any Ross Packard information (data) held on systems external to Ross Packard network. In addition, all external parties that provide services to or for Ross Packard in respect of information processing facilities and business activities, and principle information assets including the physical locations from which Ross Packard operates.

Ross Packard recognizes the important role information security plays in data protection and privacy. The potential loss or unauthorized disclosure of information has the potential to damage Ross Packard reputation and cause financial loss. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard copy form.

In order to meet these aims, Ross Packard is committed to security controls that conform to best practice and will work towards known standards, such as the ISO 27001 Information Security Management System. We carry out information security risk assessment at regular intervals in line with our Compliance Programmed. Awareness and education is provided via our Training Programmed. We keep up to date and circulate any new and relevant legal and regulatory information. Any breaches of information are recorded and reported to the relevant people and authorities. This policy and other supporting policies shall be communicated as necessary throughout Ross Packard to meet its objectives and requirements.

Mr. Ross Packard M.D has ultimate responsibility for information security within Ross Packard. Managers are responsible for information security in their own business areas, and each employee has a duty to protect information in the same way. Information will be restricted to contracted third party suppliers and other external parties to the minimal required to complete their function.

Relevant legislation in connection with this policy included, but is not limited to The EU General Data Protection Regulation (2016), The Computer Misuse Act (1990), The Data Protection Act (1998), The Regulation of Investigatory Powers Act (2000), The Telecommunications (Lawful Business Practice) (Inception of Communications) Regulations (2000), and the Freedom of Information Act (2000)

06. Relationship Management

The purpose of this policy is to establish strategic, management and operational direction and objectives for relationship management. This policy will ensure the implementation of new and existing business is adequately developed and treated. This policy applies to all contracted parties and covers the level of resource required, responsibilities, direction and guidance to ensure best practice is followed, covering operational management, quality, business continuity and information security. Periodic meetings will be held to ensure the current situation and future changes are in line with policy expectations and the spirit of our agreement.

07. Incident Management

This policy is intended to ensure that the company is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. The scope of this policy covers all information assets owned or provided by the company, whether they reside on the corporate network or elsewhere. Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, encryption and patch management; and non-technical tools such as good physical security for laptops and mobile devices. Additionally, prior to an incident, the company must ensure that staff know what actions to take when an incident is suspected and who is responsible for responding to an incident.

The company must have discussions with an IT Security company that offers incident response services before such an incident occurs in order to prepare an emergency service contract. This will ensure that high-end resources are quickly available during an incident. Finally, the company should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations. All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or unknown third parties.

First, notify Vikki Williams so the appropriate checks and communication can be carried out. Recovery will involve changing any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replacing the lost hardware and restoring data from the last backup. Notifying the applicable authorities and clients as needed if a theft has occurred and follow disclosure guidelines in accordance with the Information Commissioner's Office best practice. Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

08. Asset Management

This asset management policy provides the overall framework for the management of assets from procurement to disposal and identifies the roles and responsibilities that relate to the implementation of this policy. This policy applies to all staff that use or hold assets purchased or created by Ross Packard, including intellectual property, data sets, motor vehicles, desktops and laptops, monitors, printers and scanners, phones, mobile phones, smart phones, tablets and PDA's, servers, network switches, racks and other related equipment, desks, seating, cupboards and other forms of furniture and stationary.

The IT and Operations Managers have day to day responsibility for coordinating audit of assets, updating and maintaining the accuracy of the inventory, ensuring assets are signed for by holders before they are taken, applying asset tags before assets are taken, checking equipment is returned in the same configuration, ensuring assets are signed for when returned, looking after assets held in stock, providing reports on assets stripped for spares, creating an asset list of disposed assets, confirming disposal of assets on inventory, and marking assets lost or stolen on the inventory. Any actual or suspected breach of the asset management policy must be reported to Mr. Ross Packard, who will take appropriate action. Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

09. Vulnerability Management

The purpose of this policy is to provide guidelines that mitigate the possibility of data breaches from internal and external sources. This also looks ahead to potential future threats and trends to keep ahead of currently acceptable practice. This policy covers the entire company, clients and supply partners involved in providing our services. It sets the level of security the company wishes to maintain, guidelines for management practices, classification of risk / threat, access control and consequences for noncompliance.

The development, implementation and execution of the vulnerability assessment process is the responsibility of Ross Packard M.D. Periodic or continuous vulnerability assessment scans will be performed on all network assets deployed on company IP address space. Staff are expected to cooperate with any vulnerability assessment conducted on systems for which they are held accountable. Staff are expected to cooperate in the development of any remediation plan. Our vulnerability assessment process consists of five phases: Preparation, Vulnerability Scan, Defining Remediating Actions, Implementing Remediating Actions and Rescan.

Any vulnerability not detected after a schedule scan takes place will only be detected at the next scheduled scan. If the frequency of scans is too wide, this could leave systems vulnerable for a long period. Regular scans, or continuous vulnerability management, is scheduled to reduce the exposure time ensuring new vulnerabilities are detected in a timely manner. Any vulnerability scans or follow up activities, performed outside Ross Packard must be approved by Mr. Ross Packard M.D. Any staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and potential legal action

10. Acceptable Use

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use. This policy explains how information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked to use common sense when using company resources.

Questions on what constitutes acceptable use should be directed to the user's supervisor. Since inappropriate use of systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of information technology resources for the protection of all parties involved.

The scope of this policy includes any and all use of IT resources, including but not limited to, computer systems, email, the network, and Internet connection. Personal usage of company email systems is prohibited. Users should use corporate email systems for business communications only. The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.

The user is prohibited from forging email header information or attempting to impersonate another person. Typically, email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption. It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected. Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Confidential data must not be A) shared or disclosed in any manner to non- employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access. The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to: Engage in activity that is illegal under local, state, federal, or international law, Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company, Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media, Engage in activities that cause an invasion of privacy, Engage in activities that cause disruption to the workplace environment or create a hostile workplace, Make fraudulent offers for products or services, Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function, Install or distribute unlicensed or "pirated" software, Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

Blogging and social networking by the company's employees are subject to the terms of this policy, whether performed from the company network or from personal systems. Blogging and social networking is never allowed from the company computer network. In no blog or website, including blogs or sites published from personal or public systems, shall the company be identified, company business matters discussed, or material detrimental to the company published. The user must not identify himself or herself as an employee of the company in a blog or on a social networking site. The user assumes all risks associated with blogging and/or

social networking.

Instant Messaging is allowed for corporate communications only. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted. The Internet is a network of interconnected computers of which the company has very little control. The employee should recognize this when using the Internet and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

11. Physical Security

The purpose of this policy is to protect the company's physical information systems by setting standards for secure operations. This policy applies to the physical security of the company's information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting the company's office is covered by this policy.

Please note that this policy covers the physical security of the company's Information Technology infrastructure and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must be taken to ensure that this policy is consistent with any existing physical security policies.

When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges. At a minimum, the company's site should meet the following criteria: A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters. A site should not be located in an area where the crime rate and/or risk of theft is higher than average. A site should have the fewest number of entry points possible. If these criteria cannot be effectively met for any reason, the company should consider outsourcing its data in whole or in part to a third-party data center or hosting provider, provided that such a company can cost effectively meet or exceed the company's requirements.

At a minimum, the company will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure the company's assets. In addition to this the company must provide security in layers by designating different security zones within the building. Security zones should include: Public: This includes areas of the building or office that are intended for public access. Access Restrictions: None. Additional Security Controls: None. Examples: Reception, common areas of building. Company: This includes areas of the building or office that are used only by employees and other persons for official company business. Access Restrictions: Only company personnel and approved/escorted guests. Additional Security Controls: None. Examples: Hallways, private offices, work areas, conference rooms. Private: This includes areas that are restricted to use by certain persons within the company, such as executives, accountants, engineers, and IT personnel, for security or safety reasons. Access Restrictions: Only specifically approved personnel. Additional Security Controls: None. Examples: Executive offices, network room, manufacturing area, financial offices, and storage areas.

Access controls are necessary to restrict entry to the company premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with the company's guidelines for their use. The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that the company has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good

security can be obtained with keys and keypads. While key cards are allowable forms of access controls, the company does not require their use at this time. A security alarm system is a good way to minimize risk of theft or reduce loss in the event of a theft. The company mandates the use of professionally monitored alarm system. The system must be monitored 24x7, with company personnel being notified if an alarm is tripped at any time.

Certain physical precautions must be taken to ensure the integrity of the company's data. At a minimum, the following guidelines must be followed: Computer screens must be positioned where information on the screens cannot be seen by outsiders, Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information, Users must log on or shut down their workstations when leaving for an extended time period, or at the end of the day, Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit), Network ports that are not in use must be disabled.

In addition to protecting the data on the company's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft. In order to minimize the risk of data loss through loss or theft of company property, the following guidelines must be followed: Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured, Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the company's Mobile Device Policy for guidance, Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to the company's Confidential Data Policy for guidance.

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed: Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity. Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized. Strong magnets must not be used in proximity to company systems or media. Except in the case of a re suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto company systems. Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

It is the company's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the company's office. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall fire safety policy. Fire, smoke alarms, and/or suppression systems must be used, and must conform to local re codes and applicable ordinances. Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together. Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety. Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if practical. Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear. A smoke alarm monitoring service should be considered that will alert a designated company employee if an alarm is tripped during non-business hours. It is the company's policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general but is particularly true for minimizing risk to company systems and data. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall security policy. Identification (ID) badges are useful to identify authorized persons on the company premises. The company has established the following guidelines for the use of ID badges. Employees: Photo ID badges are required and must be displayed at all times while on company premises. Employees must

remove their badges from view when out of the office. Non-employees/Visitors: Visitor badges are required. Specific, non-generic badges must identify visitors by name and the date of the visit. The company should investigate visitor badges that automatically expire and determine if the use of such technology is feasible for use. Users must a report lost or stolen badge immediately to his or her supervisor. A temporary badge may be utilized in such cases until the badge can be re-generated. Initial badge generation will be done only at the direction of Human Resources for new hires or users changing jobs. Users must show photo identification for identity verification.

The company must maintain a sign-in log (or similar device) in the reception or entry area and visitors must be required to sign in upon arrival. At minimum, the register must include the following information: visitor's name, company name, name of person visiting, sign-in time, and sign-out time. Visitors should be given only the level of access to the company premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by the company. Examples of a trusted visitor may be the company's legal counsel, financial advisor, or a courier that frequents the office, and will be decided on a case-by-case basis.

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed. This policy will be enforced by [NAME / TITLE]. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

12. Backup

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed. This policy applies to all data stored on company systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

The company must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process. A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include: All data determined to be critical to company operation and/or employee job function, all information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server, all information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

Backup frequency is critical to successful data recovery. The company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator. Incremental: every day. Full: every 3 days.

Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. On site storage must be balanced with the time required to recover the data, which must meet the company's uptime requirements. The company has determined that backup media must be rotated offsite at least once per day. Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential company data, precautions must be taken that are commensurate to the type of data being stored.

The company has set the following guidelines for backup storage. When stored onsite, backups should be kept in an access-controlled area. When shipped offsite, a hardened facility (i.e., commercial backup service or safe deposit box) that uses accepted methods of environmental controls, including re suppression, and security

processes must be used to ensure the integrity of the backup media. Online backups are allowable if the service meets the criteria specified herein. When determining, the time required for backup retention, the company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company has determined that the following will meet all requirements (note that the backup retention policy must conform to the company's data retention policy and any industry regulations, if applicable): Incremental Backups must be saved for one month. Full Backups must be saved for six months.

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems. Backup restores must be tested when any change is made that may affect the backup system, as well as twice per year. Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

13. Server Access

The purpose of this policy is to ensure a minimum level of security is maintained by all company staff and authorized third parties that have access to the server room, to ensure data security in use and at server disposal is managed.

All servers will be hosted within the dedicated Server Room. The Server Room will have a secure perimeter. The Server Room will have access restricted by Access Control and additionally by barrel-lock keys. Access will be limited to members of IT engaged in server, network and telecommunications installation and maintenance work. All servers will be marked with an individual system tag and the server name

Environmental Controls: All servers will be protected from surges, spikes, sags or burnouts in the electricity supply by the use of Uninterruptable Power Supplies. All servers will be protected from excessively high or low temperatures by temperature control. All servers will be protected from excessively high or low humidity by humidity control. All servers will be situated in racks, raising them above ground level and therefore reducing the liability of damage through flooding. Server room air conditioning equipment will be fitted with dust filters. All environmental control equipment will be regularly maintained

Data Security: Access to applications and storage spaces shall be tightly controlled by the use of Access Control Lists. Remote access to server operating systems shall only be granted by Mr. Ross Packard M.D. User access, where facilitated, will only be provided on a basis of least privilege, tight implementation, granular access controls
and limited access to programs. Servers will, where possible, sit on a restricted subnet with access to other subnets only being granted via firewall. Normally, server operating systems will not be remotely accessed by external suppliers (see Remote Access Policy). Desktop sessions on a server will automatically lock after being active for 10 minutes. Desktop server sessions will only be available by encrypted Remote Desktop Protocol connections. As large processing jobs need to be undertaken within sessions, inactive sessions shall not shut down, nor will a restriction on connection time be imposed. The only method a session can be reconnected is by re-authentication of the appropriate user account. Server software and firmware will be patched in a timely manner. Non-critical and test systems will be patched first to test system and application operability

Controls Against Malicious Code: Anti-virus software will be installed on every server and kept up to date. All servers will sit behind firewalls. User access to server desktop environments, where required for remote desktop purposes, will be tightly controlled by the IT Manager in order to block access to system programs, tools, files and processes. User access will have no administrative rights, installation rights or privileges.

Internet Explorer will only run in Enhanced Security Configuration mode. The servers will run different anti-virus software to workstations.

Software: All software on servers must be authorized and requested by system owners. Software on servers must only be installed by Mr. Ross Packard M.D or, if granted permission in writing by the system owner, an authorized third party. All software installations, updates and removal will be subject to the company's Change Management Policy. Regular reviews of software and data content on servers classed as mission critical must be carried out. The responsibility to initiate reviews lies with Mr. Ross Packard M.D. Unauthorized software or data will be removed.

Roles and Responsibilities: It is the responsibility of Mr. Ross Packard M.D to ensure that this policy is enforced and complied with. Mr. Ross Packard M.D is responsible for holding and maintaining Access Control. All other staff with rights to access – All staff must be aware of this policy and their obligations. It is their responsibility to ensure they carry out their duties in a professional manner whilst working in the Server Room. All visitors need to be made aware of this policy and their obligations. It is the responsibility of the member of IT accompanying the visitor to ensure they carry out their duties in a professional manner whist working in the Server Room.

Access to the Server Room: A list of authorized staff managed by Mr. Ross Packard M.D. A procedure for the safe use of the Server Room will be made available. This will mainly be concerned with the safe use of the fire safety system in the room. The primary mechanism for controlling access to the Server Room is via a key-barrel door lock. There is also protection via the fire detection system. Staff must wear their identification badge at all times, and visitors must wear visitor's passes. All authorized staff are required to be signed in and out of the Server Room Access Control. This includes all visitors, who must be accompanied by a member of staff at all times. Access Control Sheets are retained by Mr. Ross Packard M.D. Inclusion onto the Server Room Access List must be approved and signed off by Mr. Ross Packard M.D. These inclusions will be documented and retained by Ross Packard M.D. Entry into the Server Room by tailgating another staff is not permitted. The use of mobile phones, pages or other equipment that emits radio waves within the Server Room is forbidden unless specific exemption is obtained from the Mr. Ross Packard MD. Food and drink must not be taken into the Server Room. On a monthly basis, Vikki Williams/ Ross Packard will review the Access Control Log. The Log will be signed at the last entry and dated.

Training and Awareness: All relevant staff will have this policy brought to their attention by Vikki Williams. The policy will also be available Secure Estimator office. Any queries regarding this document will be dealt with by Mr. Ross Packard MD

Review: This policy will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organizational change or relevant changes in legislation or guidance

Monitoring: Access into and out of the Server will be monitored by Vikki Williams via the Access Control Log. Any discrepancy with work schedules against the Access Control Log will be investigated and appropriate action will be taken. Unauthorized access into the Server Room must be reported to Vikki Williams as a breach of security. Server status and operating system performance, including system resource usage and bandwidth usage shall be monitored. Server hardware status shall be monitored. Audit logs shall record user activities, exceptions and information security events. System administrator and system operator activities shall also be logged. Logs will be held for 30 days and then deleted on a rolling basis. Audit log information is only accessible by domain administrators. Domain controller logs will be exported and held on a separate server

Backup: All company servers are backed up nightly. A different backup is taken each night. A full backup is taken each weekend. Nightly backups are stored for 1 week. Weekly backups are stored for 1 month. Monthly backups are stored for 1 year. Yearly backups are stored indefinitely. Backups are to be considered a disaster recovery measure. They are not provided to restore user-deleted data.

Hardware Warranties and Replacement: By default, all company servers are provided with 3 years' warranty. Warranties may be extended for a further two years (up to a maximum of five years from the point of purchase). Hardware failures on in-warranty servers will be subject to a 4-hour working day replacement service, after fault diagnosis and reporting has occurred. At any point of warranty expiration, physical servers

shall be replaced. Full provision must be made in company budgets to fund the replacement of servers at the point of warranty expiration. All production servers must be in warranty

Disposal: When servers are removed from service, their hard drives will be removed and degaussed before disposal. Memory will also be removed from the chassis.

14. Network Security

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the company's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies. This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by the company.

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged. The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. Logs from application servers are of interest since these servers often allow connections from many internal and/or external sources. These devices are often integral to smooth business operations. Examples: Web, email, database servers. Requirement: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs. Logs from network devices are of interest since these devices control all network traffic and can have a huge impact on the company's security. Examples: Firewalls, network switches, routers. Requirement: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.

Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any cases where this occurs, this section shall supersede. Examples: File servers, lab or manufacturing machines, systems storing intellectual property. Requirements: While logging is important to the company's network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, the company recommends that a log management application be considered. Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events, however, a member of the company's IT team should still review the logs as frequently as is reasonable. Logs should be retained in accordance with the company's Retention Policy.

Unless otherwise determined by Ross Packard, logs should be considered operational data. Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the company network through the use of a firewall. Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised. This will also prevent remote desktops from accessing the internal network.

Servers typically accept connections from several sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly

important to secure network servers.

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically act when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic. The company neither requires nor prohibits the use of IDS or IPS systems.

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the company's network security. Security testing can be provided by IT Staff members but is often more effective when performed by a third party with no connection to the company's day-to-day Information Technology activities. The following sections detail the company's requirements for security testing. Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the company's IT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network. Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of Ross Packard MD. Internal testing should have no measurable negative impact on the company's systems or network performance. External security testing, which is testing by a third-party entity, is an excellent way to audit the company's security controls. Ross Packard MD must determine to what extent this testing should be performed, and what systems/applications it should cover.

As a rule, "penetration testing," which is the active exploitation of company vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact company systems or data. The company requires that external security testing be performed twice per year.

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire company.

An employee must be designated as a manager for the company's security programme. He or she will be responsible for the company's compliance with this security policy and any applicable security regulations. This employee must be responsible for A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on the company's information security program (as detailed below), D) any ongoing testing or analysis of the company's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

A training programme must be implemented that will detail the company's information security programme to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually.

The company's security policies should be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to the company's security policies.

15. Network Access & Authentication

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards. The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to

the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the company's externally-reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup: Positive ID and coordination with Human Resources is required. Users will be granted least amount of network access required to perform his or her job function. Users will be granted access only if he or she accepts the Acceptable Use Policy. Access to the network will be granted in accordance with the Acceptable Use Policy.

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use: Accounts must be created using a standard format (i.e., firstnamelastname). Accounts must be password protected (refer to the Password Policy for more detailed information). Accounts must be for individuals only. Account sharing and group accounts are not permitted. User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function. Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed. Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of Ross Packard MD or as required by applicable regulations or third-party agreements.

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must create a process to notify Vikki Williams in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

User machines must be configured to request authentication against the domain at start-up. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network. When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the company's Password Policy.

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the company mandates additional scrutiny of users remotely accessing the network. The company's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passwords are required to be activated after 15 minutes of inactivity.

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with product that provides network admission control.

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the company network or across a public network

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password- guessing and brute-force attempts, the company must lock a

user's account after 5 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of Mr. Ross Packard MD.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

While some security can be gained by removing account access capabilities during non-business hours, the company does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the company's business requires all-hours access.

16. Virtual Private Network

This policy details the company's standards for site-to-site VPNs. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the VPN pathways into the network. The scope of this policy covers all site-to-site VPNs that are a part of the company's infrastructure, including both sites requiring access to the company's network (inbound) and sites where the company connects to external resources (outbound). Note that remote access VPNs are covered under a separate Remote Access Policy.

Site-to-site VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as Triple DES or AES. Site-to-site VPNs must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product. When site-to-site VPNs are implemented, they must adhere to the policy of least access, providing access limited to only what is required for business purposes. This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes.

The company should manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the IT Manager. Depending on the nature of the site-to-site VPN, the IT Manager will use his or her discretion as to whether additional logging and monitoring is warranted. As an example, a site-to-site VPN to a third party would likely require additional scrutiny but a VPN to a branch office of the company would likely not be subject to additional logging or monitoring.

Site-to-site VPNs are created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Encryption keys should be changed yearly. If certificates are used instead of pre-shared keys, the certificates should expire and be re-generated after three years.

17. Remote Access

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium. The scope of this policy covers all employees, contractors, and external parties that access company resources over a third- party network, whether such access is performed with company-provided or non-company-provided equipment.

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically prohibited: Installing a modem, router, or other remote access device on a company system without the approval of Vikki Williams / Ross Packard. Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from Ross Packard. Use of non-company-provided remote access software. Split Tunneling to

connect to an insecure network in addition to the company network, or in order to bypass security restrictions.

Accessing the corporate network through home or public machines presents a security risk, as the company cannot completely control the security of the system accessing the network. Non-company-provided computers are allowed to access the corporate network only with the approval of the Management Team and IT department.

The company will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. The company may evaluate this in the future, but as of the date of this policy does not wish to impose a policy on timeouts.

18. Wireless Access

The purpose of this policy is to state the standards for wireless access to the company's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points should be located central to the office space rather than along exterior walls. If it is possible with the technology in use, signal broadcast strength should be reduced to only what is necessary to cover the office space. Directional antennas should be considered in order to focus the signal to areas where it is needed.

Physical security of access points should be considered - access points should not be placed in public or easily accessed areas if possible.

If confidential data is to be accessed over the wireless network, additional security measures must be taken since the security of the wireless LAN cannot be absolutely verified. The company's remote access policy must be followed in order to provide additional encryption software (IPSec, SSL, etc.) to secure this data during wireless transmission.

Users should disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC. Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the company.

The wireless network should be periodically audited to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, and use of strong encryption.

19. Mobile Devices

The purpose of this policy is to specify company standards for the use and security of mobile devices. This policy applies to company data as it relates to mobile devices that can store such data, including, but not

limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with company data.

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The company should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following: Laptop locks and cables can be used to secure laptops when in the office or other fixed locations. Mobile devices should be kept out of sight when not in use. Care should be given when using or transporting mobile devices in busy areas. As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the boot, with the interior boot release locked; or in a lockable compartment such as a glove box. The company should evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable. The company should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defence for protecting company data. The following sections specify the company's requirements for data security as it relates to mobile devices.

At a minimum, company data must be stored on an encrypted partition. Whole disk encryption should be considered if the data is especially sensitive. Laptops must require a username and password for login.

Use of encryption is required on PDAs/smart phones if data stored on the device is especially sensitive. PDAs/smart phones must require a password for login.

This section covers any USB drive, ash drive, memory stick or another personal data storage media. Storing company data on such devices is not permitted under any circumstance. No company data can be stored on personal media players.

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

Users are prohibited from connecting company-provided computers to any network other than the company's network. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the company.

The following guidelines apply to the use of mobile devices: Loss, theft, or another security incident related to a company-provided mobile device must be reported promptly. Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device, it must be appropriately secured and comply with the Confidential Data Policy. Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy. Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA, but this must be passcode or pin protected and encrypted wherever possible.

The company must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices should be taken and audited against this policy on a periodic basis.

20. Cloud Computing

This cloud computing policy is meant to ensure that cloud services are NOT used without Vikki Williams / Ross Packard knowledge. It is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-

owned data. This is necessary to protect the integrity and confidentiality of company data and the security of the corporate network.

The company remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby employees can use cloud services without jeopardising company data and computing resources.

This policy applies to all employees in all departments of the company without exception. This policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact [NAME / TITLE] for further information and guidance.

Use of cloud computing services for work purposes must be formally authorised by Vikki Williams / Ross Packard, who will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by Vikki Williams/ Ross Packard. The use of such services must comply with company existing Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy/CREST Policy/Information Security Policy. Employees must not share log-in credentials with co-workers. The IT department will keep a confidential document containing account information for business continuity purposes.

The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the company. Vikki Williams/ Ross Packard decides what data may or may not be stored in the Cloud. Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data pre-approved cloud computing services.

21. Third Party Connection

The policy is intended to provide guidelines for deploying and securing direct connections to third parties. The scope of this policy covers all direct connections to the company's network from non-company owned networks. This policy excludes remote access and Virtual Private Network (VPN) access, which are covered in separate policies.

Third party connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third-party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the Ross Packard.

Third party connections require additional scrutiny. The following statements will govern these connections: Connections to third parties must use a firewall or Access Control List (ACL) to separate the company's network from the third party's network. Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible, this should include time-of-day restrictions to limit access to only the hours when such access is required. Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources. If a third-party connection is deemed to be a serious security risk, the IT Manager will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the IT Manager.

Best practices for a third-party connection require that the link be held to higher security standards than an intra-company connection. As such, the third party must agree to: Restrict access to the company's network to only those users that have a legitimate business need for access. Provide the company with the names and any other requested information about individuals that will have access to the connection. The company reserves the right to approve or deny this access based on its risk assessment of the connection. Supply the company

with on-hours and off-hours contact information for the person or persons responsible for the connection. (If confidential data is involved) Provide the company with the names and any other requested information about individuals that will have access to the company's confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

In order to ensure that third-party connections are in compliance with this policy, they must be audited periodically. This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

22. Outsourcing

The purpose of this policy is to specify actions to take when selecting a provider of outsourced IT services, standards for secure communications with the provider, and what contractual terms should be in place to protect the company. This policy covers any IT services being considered for outsourcing.

Outsourcing IT services is often necessary but should be carefully considered, since by nature a certain amount of control will be lost by doing so. The following questions must be affirmatively answered before outsourcing is considered: Can the service be performed better or less expensively by a third-party provider? Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house? Will outsourcing the service positively affect the quality of this service? Is the cost of this service worth the benefit? Are any risks associated with outsourcing the service worth the benefit?

The company permits the outsourcing of critical and/or core functions of the company's Information Technology infrastructure as long as this policy is followed. Examples of these types of functions are data backups, remote access, security, and network management. Once the decision to outsource an Information Technology function has been made, selecting the appropriate provider is critical to the success of the endeavor.

Due diligence must be performed after the potential providers have been pared to a short list of two to three companies. Due diligence must always be performed prior to a provider being selected: If the outsourced service will involve the provider having access to, or storing the company's confidential information, due diligence must cover the provider's security controls for access to the confidential information, and, the outsourcing contract must provide a mechanism for secure information exchange with the service provider.

This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange. The company and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to company data.

The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited.

23. Supplier Due Diligence

Ross Packard Paintwork use a checklist to ensure compliance with new suppliers and effective practice of existing partnerships. Ross Packard Paintwork requires that all arrangements between itself and suppliers are confirmed in legally binding contracts. All contracts, whether they are called service level agreements or contracts, need to include some mandatory clauses. Legally binding agreements are drafted and checked by legal advisors. Tax and accounting implications of each contract is checked by Vikki Williams/Ross Packard.

Our due diligence checklist identifies key factors to consider before entering into a contract. They are drafted from the point of view of Ross Packard Paintwork, but they also tell suppliers what they should expect will be reviewed and checked by Vikki Williams / Ross Packard. Suppliers are made aware that they may like to consider to what extent Vikki Williams/ Ross Packard complies with the conditions of the due diligence checklist.

The scope and depth of the due diligence carried out is proportionate to the size and complexity of the contract and the level of risk. Vikki Williams / Ross Packard will look at publicly available ratings from industry bodies and previous performance in terms of outcomes and finance. It is the responsibility of the Ross Packard Paintwork director or manager to satisfy themselves that the supplier has been selected fairly through an open and transparent process, and has sufficient capacity, capability, quality and business standing to deliver the provision that is being offered. The checklist is used as a guide in reaching this conclusion and a copy of this checklist can be provided upon request.

24. Passwords

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy to understand policy is essential.

The purpose of this policy is to provide guidelines for use of passwords and will help users understand why strong passwords are necessary – helping to create passwords that are both secure and useable. This policy applies to any person provided with a user account on our company network or systems, including employees, guests, contractors, partners, vendors, etc. Historically, system usernames and passwords have been issued by Ross Packard Paintwork and exchanged point to point via agreed Data Controllers. Latterly, steps have been made to introduce an advanced password management approach where the user sets their own password with reset request at 90 days.

The best security against a password incident is to follow a sound password construction strategy. Ross Packard paintwork strongly suggests users adhere to the following guidelines on password construction. Passwords should: be at least 8 characters, be a mix of letters, numbers and special characters (punctuation marks and symbols), be a mix of upper and lower-case characters, not utilize words that can be found in a dictionary, not be an obvious keyboard sequence (i.e., qwerty), Not include “guessable” data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Passwords should be considered confidential data and treated with the same discretion as any of the company’s proprietary information. The following guidelines apply to the confidentiality of passwords. Users should not: disclose their passwords to anyone, share their passwords with others (co-workers, supervisors, family), write down their passwords or leave them unsecured, check the “save password” box when authenticating to applications, use the same password for different systems and/or accounts, send passwords via email, re-use passwords in order to maintain good security passwords should be periodically changed. This limits the damage a hacker can do as well as help frustrate brute force attempts.

At a minimum, users must change passwords every 90 days. Companies may use software that enforces this policy by expiring user passwords after this time period. On termination of user employment all access to the company’s systems and external systems will be revoked. All passwords relating to the company and external system access should be passed to the line manager

25. Encryption

The protection of information and access to storage systems is vitally important. Protecting personally identifiable and business critical information from unauthorized access, disclosure or loss whether by theft or accident is of paramount importance. All steps must be taken to protect this information.

Encryption technologies provide a level of protection for the storage, transmittal, retrieval and access to this data. Encryption works by converting data to make it inaccessible and unreadable to unauthorized individuals. The only way to read the encrypted data is by using a decryption key.

The Data Protection Act requires Ross Packard Paintwork to have appropriate policies and procedures in place to ensure the safe keeping, use, retrieval and access to data. We have a responsibility to protect the data we hold.

The General Data Protection Regulations encourage 'Privacy by Design' and the incorporate an end to end security principle. Demonstrating good security standards minimizes risk. If a breach occurs and the data is securely encrypted is it not mandatory to inform Data Subjects provided the information cannot be accessed.

The purpose of this policy is to: Provide guidance that limits the use of encryption to algorithms that have been proven to work effectively, Provide direction to ensure regulations are followed, Detail the specification and deployment of data encryption software, Provide guidance on the responsibilities of the use and handling of portable media, Provide clarity on the types of portable storage and mobile devices which are allowed for use, Describe how encryption will be used and applied to devices, Provide guidance on the responsibilities of the use of encrypted devices, Detail the method of reporting breaches of this policy, whether intentional or accidental

This policy applies to all employees and affiliates and covers all electronic data and devices irrespective of whether or not the data held on them is considered sensitive or confidential. Encryption covers the following devices and applications: Servers, desktops and laptops - Handheld devices such as mobile phones, smart phones and tablets - Storage devices, such as memory sticks and external drives - Removable media such as DVD's and back up tapes – Website - Email

The encryption software employed for use at Ross Packard Paintwork uses the Advanced Encryption Standard 256 bit, as set out in the IETF/IRTF Cipher Catalogue and FIPS 140-2. Email security using TLS on all mail traffic with enforced TLS recommended for all emails sent and received to specific domains to allow encryption policies to be guaranteed. We are looking to enforce TLS with all partners so we can ensure both sent and received email are encrypted with TLS.

The encryption software employed for use at Ross Packard Paintwork uses the Advanced Encryption Standard 256 bit (SHA256 bit key). Full disk encryption is used where applicable such as laptops that are used outside the office. Local client PC's such as desktops are not permitted to store any private data and must use private shared drives with authentication using local active directory credentials.

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise. Key generation must be seeded from an industry standard random number generator.

26. Recertification

Recertification simplifies and automates the process of periodically revalidating a target type (account or access) or a membership (role or resource group). The recertification process validates whether the target type or membership is still required for a valid business purpose. The process sends recertification notification and approval events to the participants specified. A recertification policy includes activities to ensure that users provide confirmation that they have a valid, ongoing need for a specified resource or membership. An example of this would be an Account Manager's online view of a client Management Report. The purpose of this policy is to define how frequently users must certify their need for a resource or membership. This policy also defines the operation that occurs if the recipient declines or does not respond to the recertification request. Recertification policies use a set of notifications to initiate work ow activities that are involved in the recertification process.

This policy applies to all staff, clients, suppliers and associated interested parties that have authorized access to company information systems. All changes are the responsibility of the agreed System Administrator or Data Controller. The process is as follows: The System Administrator will produce a system-generated list of all user accounts, and their levels of access, From the system-generated list, the System Administrator will select user accounts to be recertified, The System Administrator will cross-check names with access request/ authorization to confirm that an appropriately authorized reference is on file for each user, and that the

employee's or other authenticated user's level of system access are appropriate, The System Administrator will send the list to the users' supervisors for review and recertification, The System Administrator will take appropriate action to modify or terminate user accounts, as indicated by User Account Recertification results, The System Administrator will prepare a report of User Account Recertification results, corrective actions and supporting documentation (User Account Recertification Report) for review and approval by the System Owner, The System Owner will review and sign User Account Recertification Reports to verify the results of the recertification and that appropriate corrective actions were taken. If weaknesses in the user account controls for the system are discovered, appropriate remediation will be pursued, The System Administrator will retain all User Account Recertification documentation for 7 years. Documentation will be retained and disposed of by calendar year (no incremental disposal), At no time will usernames and passwords be shared with the user's supervisors. Usernames and passwords will be initiated by the Data Controller and changed by the user at the point of recertification, on termination of user employment all access to the company's information systems and accounts will be revoked. All passwords relating to the company and external system access will be removed

27. Data Retention (including record retention)

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organization.

The purpose of this policy is to specify the company's guidelines for retaining different types of data. The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry, or UK / EU regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

The company does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective and would place an excessive burden on staff to manage the constantly-growing amount of data. Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include: Litigation, Accident investigation, Security incident investigation, Regulatory requirements, Intellectual property preservation

This section sets guidelines for retaining the different types of company data. Personal: There are no retention requirements for personal data. In fact, the company requires that it be deleted or destroyed when it is no longer needed. Public: Public data must be retained for 1 year. Operational: Most company data will fall in this category. Operational data must be retained for 2 years. Critical: Critical data must be retained for 3 years. Confidential: Confidential data must be retained for 3 years.

The General Data Protection Regulations State: Personal Data shall be 1) Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal Data is Processed. 2) Personal Data must not be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of the appropriate technical and organisational measures required by this Regulation, in order to safeguard the rights and the freedoms of the data subject.

Data minimisation is required as per the General Data Protection Regulations 2016 principle 3 which states data must be limited to what is necessary.

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company

will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

In connection with Data Retention, a Record or Document Retention Policy establishes and describes how a company expects its employees to manage company data from creation through to destruction. It can be incorporated into an employee handbook or used as a standalone policy document.

The purpose is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed or are of no value are discarded safely at the proper time. This Policy is also for the purpose of aiding employees in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft office or other formatted files.

Below is a Record Retention Schedule that is approved as the initial maintenance, retention and disposal schedule for physical records and the retention and disposal of electronic documents. Managers are in charge of the administration of this policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Senior Administrator is also authorized to make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with current legislation and includes the appropriate document and record categories for monitoring current legislation affecting record retention, annually review the record retention and disposal program, and monitoring compliance with this policy. This policy applies to all physical records generated, including both original documents and reproductions. It also applies to the electronic documents described above.

Record Type	
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years
Annual Plans and Budgets, Bank Statements and Cancelled Cheques	7 years
Employee Expense Reports, General Ledgers, Interim Financial Statements	7 years
Notes Receivable ledgers and schedules Investment Records	7 years
Credit card records (documents showing customer credit card number)	7 years

28. Data Destruction

This policy sets out the requirements for staff regarding the secure disposal of IT equipment and information. Secure disposal means the process and outcome by which information including information held on IT equipment is irretrievably destroyed in a manner which maintains the security of the equipment and information during the process and up to the point of irretrievable destruction. IT equipment means all equipment purchased by or provided to store or process information including but not necessarily limited to desktop computers, servers, printers, copiers, laptops, tablet computers, electronic notebooks, mobile telephones, digital recorders, cameras, USB sticks, DVDs, CDs and other portable devices and removable media. Information means all information and data held or recorded electronically on IT equipment or manually held or recorded on paper.

For the purpose of this policy, the information held can be divided into two categories: non-sensitive; and sensitive information. Sensitive information comprises: all personal information and all confidential information, the loss of which would, or would be likely to, cause damage or distress to individuals. The default category is that all information is deemed to be sensitive unless specifically identified as otherwise.

It is the responsibility of all staff to ensure that the information held is disposed of appropriately and that all sensitive information is disposed of securely.

Responsibility for this policy resides with Vikki Williams/ Ross Packard. This policy on disposal covers all data or information held whether held digitally or electronically on IT equipment or as manual records held on paper or in hard copy. It is our policy to ensure that all information held is disposed of appropriately, in conformity

with our legal obligations and in accordance with regulations and Records Retention Policy. In particular, it is our policy to ensure that all sensitive information which requires disposal is disposed of securely.

Where information is held on IT equipment, such equipment will be assumed to hold sensitive information and that all information residing on such equipment must be disposed of securely. We support policies which promote sustainability and take account of environmental impact. We therefore support recycling or sustainable redeployment in the disposal of IT equipment as long as information held on the equipment is irretrievably and securely destroyed prior to the disposal of the equipment.

IT equipment must also be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006. Software must be disposed of in line with copyright legislation and software licensing provisions.

Information and data held in paper or hard copy which contain sensitive information shall be irretrievably destroyed in a way in which the information cannot be reconstituted, by shredding, pulping or incineration. The process leading to and the process of shredding, pulping or incinerating such information shall be carried out securely. Where the shredding or incineration are carried out on our behalf by a third party, there shall be a contract with that third party which appropriately evidences that party's obligations to keep that data confidential and that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

Where hard copy information is stored externally by a third-party data storage contractor, the contract shall ensure secure disposal of the data at a time which conforms with our Retention Schedule. Since the policy default is that all IT equipment which stores or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.

Where an overwrite, procedure fails to destroy the information irretrievably, the equipment shall be physically destroyed to the extent that the information contained in it is also irretrievably destroyed. For the avoidance of doubt, removable digital media including but not limited to CDs, DVDs, USB drives, where the default is that they contain sensitive data, shall, if not successfully overwritten, be physically destroyed to the extent that all data contained in the media are irretrievable. All IT equipment awaiting disposal must be stored and handled securely.

Where the overwriting procedure and/or physical destruction of IT equipment are carried out on our behalf by a third party, there shall be a contract with that third party which appropriately evidences: that party's obligations to keep that data confidential and; that party's responsibility under the GDPR for the secure disposal of the data.

In any case where IT equipment is to be passed on by Ross Packard Paintwork for reuse, those staff involved in the sale or transfer of the equipment shall ensure that any information on the equipment has been irretrievably destroyed and that any other appropriate issues, including, but not limited to, the safety of the equipment are satisfactorily addressed.

Photocopiers and printers used or owned by the company may have a data storage capacity. Where such IT equipment contains information or data, the disposal of such equipment must have due regard to this policy. Any third party contracted to dispose of sensitive hard copy information shall certify the irretrievable destruction of the information. Staff who have responsibility for the information which is disposed of shall ensure that the disposal conforms with our Records Retention Policy and Retention Schedule and that, where necessary, a record is kept documenting the disposal.

Where the disposal involves the disposal of IT equipment, Ross Packard shall keep a record of the asset number of the equipment which has been disposed of along with a record of the process by which the information stored on the equipment has been irretrievably destroyed.

All staff and other users of information should report immediately to the Office Manager any observed or suspected incidents where sensitive information has or may have been insecurely disposed of.

Staff holding Ross Packard Paintwork data in hard copy should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held. In determining whether and when the data should be disposed of, staff should consult our Retention Schedule.

It is good practice to shred, pulp or incinerate all data which requires destruction. Where hard copy waste is sensitive data it should always be securely and irretrievably destroyed by shredding, pulping or incineration. Where sensitive data are stored under contract externally, staff responsible for the contract should ensure the contract includes secure, certificated destruction of the data in accordance with the appropriate retention period.

Staff holding data on IT equipment should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held. In determining whether and when the data should be disposed of, staff should consult our Retention Schedule.

Where a decision has been made that data held on IT devices or media should not be retained, the files containing the data should be deleted from those devices. Deletion involves putting the information "beyond use" by the user of the device or media. Data held in a recycling "bin" on the device or data which can easily be recovered by the user are not regarded as being "beyond use" and may still be subject to discovery and disclosure under information law (Freedom of Information, Subject Access Request) or litigation. Staff shall never dispose of IT equipment (devices or media) without taking steps to ensure the irretrievable deletion of data held on the equipment.

Electronic or digital data which have been put "beyond use" by users may still be reconstituted by IT specialists or by forensic computer analysts. This means that when IT equipment (devices or media) are disposed of, the data should be irretrievably destroyed by being overwritten in accordance with the appropriate industry standard, or the hard disc containing the data within the equipment or the media containing the data (e.g. CD, USB stick) should be physically destroyed. Ross Packard Paintwork has shredding machines available which can destroy CDs and DVDs as well as shred hard copy.

Staff should also be mindful that mobile telephones contain data which will need to be extracted or deleted from the device before the device is disposed of. The telephone should be returned to initiate the secure return and disposal of the device.

While Ross Packard Paintwork supports the recycling or sustainable redeployment of IT equipment, staff shall not arrange for such a process without consulting the Office Manager for the proposed recycling and ensuring that any data held on the equipment are securely and irretrievably destroyed.

29. Data Classification

All employees who come into contact with sensitive information are expected to familiarize themselves with this data classification policy. Sensitive information is either Confidential or Restricted information, which can be, for example, a person's religious belief or political views. Although this policy provides overall guidance, to achieve consistent information protection, employees are expected to apply and extend these concepts to the needs of day-to-day operations. This document provides a conceptual model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

Data classification is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect information from unauthorized disclosure, use, modification, and deletion.

This data classification policy is applicable to all electronic information. Each of the policy requirements set

forth in this document are based on the concept of need to know. If an employee is unclear how the requirements should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.

The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

Access to sensitive information must be provided only after the written authorization of the Data Owner has been obtained. Access requests will be presented to the data owner using Data Access Request template. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the relevant Data Owner in accordance with a system review schedule approved by the person in charge of Information Services.

Further detail on personal data and sensitive personal data can be found in our Information Audit

30. Data Confidentiality

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

The purpose of this policy is to detail how confidential data should be handled. This policy lays out standards for the use of confidential data and outlines specific security controls to protect this data. The scope of this policy covers all company-confidential data, regardless of location. Also, covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

Confidential data must be destroyed in a manner that makes recovery of the information impossible. imply reformatting a drive does not make the data unrecoverable. The company should consider using the most secure commercially-available methods for data wiping.

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data: Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential." Users must only access confidential data to perform his/her job function. Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information. Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor. Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

Strong Encryption. Strong encryption must be used for confidential data transmitted external to the company.

Network Segmentation. Separating confidential data by network segmentation is not required but encouraged.

Authentication. Strong passwords must be used for access to confidential data.

Physical Security. Systems that contain confidential data should be reasonably secured.

Printing. When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others.

Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential.

Emailing. Confidential data must not be emailed outside the company without the use of strong encryption.

Mailing. If confidential information is sent outside the company, the user should consider using a service that requires a signature for receipt of that information.

Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.

Confidential data should be removed from documents unless its inclusion is absolutely necessary. If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

The following list is not intended to be exhaustive but should provide the company with guidelines on what type of information is typically considered confidential.

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Company financial data (if company is closely held)
- Sales forecasts
- Product and/or service plans, details, and schematics,
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party

31. Risk & Control Assessment

Evaluation of risk relating to Ross Packard Paintwork information security requirements is typically performed by senior management with varying degrees of formality. Ross Packard Paintwork has identified several information security risks that require control, which will be achieved by:

1. Ensuring intellectual property rights are protected
2. Ensuring strong business continuity, disaster recovery and reliability
3. Ensuring personal and sensitive personal data remain protected, secure and adequately managed
4. Ensuring systems and data are secure from misuse, cyber-attack and new disruptive technology
5. Ensuring systems and data are secure from security breach
6. Creating products and services that are built with security in mind

Details of Ross Packard Paintwork IT risks can be found in our Risk and Control Assessment.

32. Information Security Audit

Over the past few years, the importance of effectively managing risk has become widely accepted. An information security program is a critical component and provides the means for protecting Ross Packard Paintwork digital information and other critical information assets.

The following provides guidance for IT managers preparing for successful information security audit. Checklists and self- assessment can help identify opportunities for system and process improvements that can be performed in advance of external audit. This audit checklist and self-assessment approach encompasses all internal and external areas where information is exchanged. It is necessarily to ensure all risks of exposure are identified. Historically, information security audits have focused on the enterprise infrastructure. Increasingly, however, audits also have a significant external component. A cross functional information security risk assessment should be completed to support internal audit to act as terms of reference. Consideration is also to be given to continuous audit of key systems and transactions.

Ross Packard Paintwork must provide oversight at a level above business managers. Ross Packard Paintwork also has a role in establishing and overseeing security policy and defining the corporate security culture – which includes security assurance and ethics attitude. Manages must ensure information security efforts are supported and understood across Ross Packard Paintwork, demonstrating by example the mandate of security policies. Staff and managers must have a voice in the design of information security programs to sure they are appropriate. These are the things auditors like to see:

1. Good management practices: planning, direction, monitoring, reporting, etc.
2. Proactive management, including frequent operational monitoring
3. Supervisory review of key performance reports
4. Supervisory review of operating results (especially exception reports and analysis)
5. Organized, clear and up to date documentation
6. We documented policies and procedures
7. Managerial actions based on facts, not habits
8. A documented chain of command, roles, accountability, and responsibility
9. Consistent adherence to policy and procedures, from senior management through front line staff
10. Staff management, development, assurance that absences do not compromise controls or staff turnover
11. A balance between short and long-term focus, for both objectives and results
12. Managerial willingness to embrace new ideas

Auditors Don't Like....

1. Interviewing defensive or uninformed managers or executives
2. Wading through piles of disorganized analysis
3. Managers who can't or won't comprehend the level of risk they are incurring
4. The opposite of the 'Want to See' items listed above

Self-assessment audit results are available to external auditors upon request.

33. Change Management & Version Control

Operational change management brings discipline and control to organizations. Attention to governance and adopting formal policies and procedures will ensure more efficient infrastructure and success. Communication of this work includes documentation of important process work flows, personal roles and alignment of automation tools where appropriate. Ross Packard has formulated a Change Management and Control Policy to address the opportunities and associated risk.

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as: Contractual breach, Information being corrupted or destroyed, Computer performance being disrupted and or degraded, Productivity losses being incurred, and Exposure to

reputational risk

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

In order to fulfil this policy, the following statements shall be adhered to: The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented.

A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel.

A risk assessment shall be performed for all changes and, dependent on the outcome, an impact assessment should be performed. The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

All change requests shall be prioritized in terms of benefits, urgency, effort required and potential impact on operations.

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process, which includes contractual amendments.

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorized user; the impact assessment was performed and proposed changes were tested.

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

Implementation will only be undertaken after appropriate testing and approval of stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to e ort required to develop and implement said changes.

Version History