

Introduction

To transfer a company to digital format and fully comply with modern data protection and security laws and practices, to help maintain security through policies and guidelines that would outline the acceptable and unacceptable behaviours of employees in the workplace, outlining required compliances as these policies function as law, therefore penalties, judicial practices and sanctions will also be outlined within these policies. These policies will ensure that they are appropriate and fairly applied to everyone within the organisation, and to fully comply to modern data protection and security laws and practices.

Data security is a vital part of a business's defence against cyber-crime. To protect

against cyber-crime a plan of defence needs to be put into place and executed to help protect the company and its assets. The proposal will meet current regulatory and legislative obligations and comply to ethical and professional issues that will apply to this organisation.

Small businesses and organisations are subject to cyber-attacks, hacks and/or are held for ransom, these are ever increasing, and the threats are real. The proposal will outline details of the options available for the company's data protection. It will look at what will need to be put into place to stop cyber-attacks and help secure the companies data assets.

Suitable Position

The proposal is for setting up, applying, and implementing a secure infrastructure of cyber security protection that will protect the company against cyber-crime, cyber-threats, and insider threats.

Law *"The principles and regulations established in a community by some authority and applicable to its people, whether in the form of legislation or of custom and policies recognized and enforced by judicial decision."* [1]

Ethic *"The body of moral principles or values governing or distinctive of a particular culture or group"* [2]

The main differences between "Law" and "ethic" are that law is governed and enforced by the state whereas ethics is a moral judgement and based on cultural mores.

What is security?

Security is the protection from those who would do harm intentionally or otherwise to assets,

resources, and people. The foundation for computer and data security was developed from the concept of the computer security industry called the C.I.A triad.



Fig 1.0 C.I.A Triad [3]

The triad comprises of three principles Availability, Confidentiality, and Integrity. This has been the cornerstone for computer security industry since the start of framework. This is shown in fig 1.0.

- Availability - Enables authorised users, access to systems, applications and data and makes sure that these are running correctly and available without interference or obstruction to access when needed. [4] [5]
- Confidentiality – Ensures that only authorised users have access to the systems and its data. It is the protection from disclosure or exposure to unauthorised systems or individuals. [4] [5]
- Integrity - when the quality of data, information is uncorrupted, whole and complete it has integrity. Integrity is to ensure that the data is trustworthy and that it has in no ways been tampered with or corrupted in any way. [4] [5]

The C.I.A is now seen to be inadequate in today's constantly changing environment in security. Other models have since been adapted and utilized using the C.I.A as a foundation, one such model is the CNSS security model which was created by John McCumber in 1991 called the McCumber cube this is shown in fig 1.1. [5]

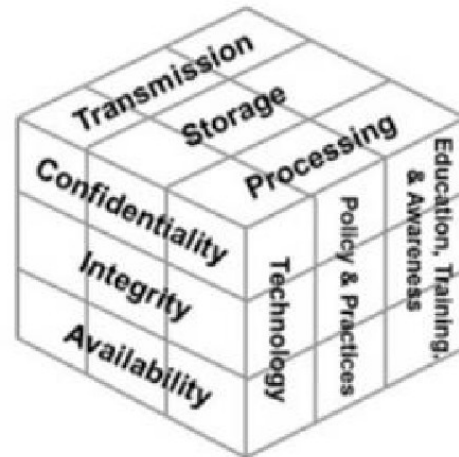


Fig 1.1 The McCumber Cube. [6]

The McCumber cube is described to be a multi-faceted, three-dimensional approach to evaluating the security of networks. The 3x3x3 cube becomes a 27-cell approach to areas of security that would need to be addressed, these are looked upon as goals for a security approach to be effective for an organisation. The McCumber cube is an expansion of the CIA which has been expanded and dimensions added to each pillar of the CIA, this approach facilitates a more complete and nuanced view of data security. The McCumber cube will help the security team to put in place the security policies and procedures needed for the organisation to have an overall security framework model. [5] [6]

The Data Protection Act 2018 is the UK's implementation of The GDPR (General Data Protection Regulation) and it states that "*The Data Protection Act applies to any business or person who uses or holds personal data on individuals within the EU and United Kingdom. Breaches of the legislation are criminal offences and can result in severe penalties*". [7]

The UK GDPR sets out seven key principals these are:

1. Lawfulness, fairness, and transparency.
2. Purpose limited.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality.
7. Accountability. [7]

They must also make sure that the information that they hold is:

- "*used fairly, lawfully and transparently*".
 - "*used for specified, explicit purposes*".
 - "*used in a way that is adequate, relevant and limited to only what is necessary*".
 - "*accurate and, where necessary, kept up to date*".
 - "*kept for no longer than is necessary*".
 - "*handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage*". [7]

For the organisation to comply with current laws and legislation a new security structure would need to be in place to ensure the correct structure is conformant to laws and safeguard the company as well. A new security department would need to be in place to ensure that the set up of the infrastructure of the new department is set and easy to maintain to reduce future costs. As the company has a large customer and supplier base the data of these information would be the company's responsibility to safeguard keep them safe from being exposed or used in criminal acts or harm. The Committee of National Security Systems (CNSS) defines information security as "*the protection of information and its critical elements, including the systems and hardware that use, store and transmit the information*". [5]

To take on the task would first be to create a team, look at the physical structure and then implement all security features to help secure the data. This is also to ensure that the company is prepared for the threats that it could face these can include, Data Breach, theft, sabotage or vandalism, software attacks, information extortion, technical software or hardware failures, human errors, espionage or trespass, compromises to intellectual property, deviation in quality of service, and forces of nature. These threats can be minimised and protected against by having a solid security framework. [5]

The roles and responsibilities of the proposed team from top down

Chief information officer (CIO)- A high ranking senior executive, critical leadership role that demands a very high knowledge of IT resources and business management skills. The responsibilities would include overseeing the organisations computing technologies, advising the CISO, strategic planning that affects the management of the information in the organisation, develops tactical and operational plans to enable the planning and management of information systems, these are accomplished with support from subordinate managers within the team. They would also be managing and directing the IT workforce and help to map out both the ICT policies and strategies for the organisation. [5]

Chief information security officer (CISO) – An executive who would be responsible for the organisation's information and data security. The CISO would oversee the security team, responsible for the security operations of the organisation, would analyse and triage immediate and possible threats, would advise the organisation with regards to potential security risks arising from changes or business moves, the CISO would keep up to date of all trending security risk and threats and implement systems or programs relevant to preventing these threats, would help to set up the identity and access control of the organisation ensuring internal staff do not abuse or misuse the data or access privileges. The CISO Other responsibilities would include assessment, the management and

implementation of the information security. Creating and implementing policies that are kept up to date and relevant to the organisation, will ensure that the security structure is clear, understandable, and relevant to the organisation, from a security standpoint. The CISO would make sure that all the above duties and initiatives run smoothly. will report to the CIO. [5]

IT security manager – A cyber security manager that would overlook the organisations cyber security programs, responsible for developing and implementing security policies, protocols, and procedures, would oversee the security systems, setting up and managing the firewalls, data protection controls, vulnerability scanning and pen testing, patching and encryption of the network and IT and security systems, this would be done by scanning alerts and logs on a daily basis and putting in place measures to protect any breaches to the security, would keep all software and tools up to date and ensure that they are working correctly, work with other departments within the organisation to keep all staff up to date with training and ensure all staff are following the policies and procedures put in place to safeguard the organisations security and data information. The IT security manager would be responsible for annual audit coordination, budgeting, and monitor expenses, recruiting, training and supervising security officers and guards. Reporting to CISO. [5]

IT information system manager – The primary role would be to manage, design, implement and monitor the information system within the

organisation. Would oversee the planning, installing and maintenance of hardware and software including upgrades to ensure that the system is always reliable and secure. Other responsibilities include responding to security breaches, running regular checks on the network and data security of the organisation, investigating, and managing threats, executing measures to mitigate threats, designing training programs and workshops for employees. [5]

Policies and Procedures

Once the team is organised policies would need to be devised and reasonable controls and safeguards are implemented. These policies will ensure the company meets requirements set out under the GDPR. The policies that will be included would enable the organisation to conform to the policies and procedures and enable the organisation to comply to the current regulations and best practices for information and data security. Policies will also ensure the organisation is fully capable of protecting the information of its customers, staff, and all other parties' information that it holds. Failure to comply to these policies could result in disciplinary, termination of contract and/or legal action taken by the organisation.

1. Acceptable use policy (example policy can be seen in the appendix) – This policy will outline that employees, members, and outside agencies know the boundaries of the use of IT equipment and services provided by and in relation to the organisation, and to safeguard and protect data and information that it holds.

This policy will outline uses relating to and including: [8] [9]

- a) Password policy – All accesses to the organisations systems and data would be through user ID's and passwords. This would be to ensure staff can access the organisations system and remotely if working from home or offsite, and through Roll Based Access Control staff would be only able to access system and data related to their job role within the organisation. This would also outline that it is the employee's responsibility to ensure that their user ID and password are always kept safe and secure. This policy outlines the organisations responsibilities and the employee's responsibilities related to passwords and their protection. It states that the organisation will establish a standard for creating strong passwords and the frequency of password changes. [8] [10]
- b) Hardware use policy – States that all ICT equipment provided by and used by the employee's, members and other agencies remains the property of the organisation and should be returned to the organisation if it becomes defective, or it is no longer required, this could be due to role change or end of employment. It also stipulates that no data should be copied in any manner without express authorisation from the organisation, and no peripheral devices

of any kind are to be connected to or used on any organisational devices without express consent. [8]

c) Internet usage policy - Use of the internet states that the access to the internet is provided by the organisation to assist employees to perform their duties and should be limited to organisational business. This policy would provide employees with the rules and regulations set out by the organisation to the appropriate use of its equipment, its network and internet access. Having this policy in place and training employees would safeguard the organisation and the employees. This policy provides the dos and don'ts whilst using the internet during office hours to reduce security risks and threats that may occur due to employee negligence. [8]

d) Access control policy – This policy will help the organisation control the access given to staff and visitors to the site, it will outline the requirements that specify how the access is managed and who may access what information. This policy will also outline the role-based access control (RBAC) which would outline the access that would be granted to employees depending on the role within the organisation. [8] [11]

e) Incident response policy- This policy will outline the steps to be taken when an incident related to security happens. It will

outline the people responsible to respond to the incident and deal with aftermath of that incident. This policy will outline the steps that would be taken after the incident, the steps required to recover quickly from the incident and the steps that would be taken to ensure that preventative measures are put into place. [12]

f) Remote access policy – This policy will provide a clear understanding of the organisations directions on how to connect to the network, its systems, software, and data securely from home or when travelling. This would be done through a VPN, restricted access through access control, and through monitoring. [8]

g) Email/communication policy (an example policy is available in the appendix) – This policy will outline the use of the organisations email system; it will outline what the organisation deems as acceptable or not acceptable use of its email system. This policy will apply to all employees, vendors and agents who access the system. [8] [13]

h) Network security policy- outlines network traffic usage, how to safeguard the network, its contents and its users against losses and damages, resources and threats, defines network uses and responsibilities, and outlines security action plans when violated. [8]

The steps that would be taken to ensure a suitable security framework.

Risk assessment, risk management, Physical security, policies, data security, and security management. Through these the organisation will be able to identify potential risks and challenges to its data and produce relevant solutions.

Building Security - First would be to run through a building risk assessment to identify potential security breaches. Ensure that the building is secure with adequate security features, this will include, walls, fencing and gates, alarms and alarm systems, interior walls and door, computer rooms and wiring closets. [5]

security cameras this will be to ensure that all people who are within the organisations grounds are meant to be there or have permission to be there, this can also help towards identifying unwanted visitors or trespassers, security guard/s will be the first point of contact who will make sure all people and vehicles coming into the property have security clearance to do so, this may be through ID cards and number plate recognition cameras, visitors ID cards can be issued with limited access rights. Guard dog/s will be used to secure the grounds and checking visitors and delivery vehicles as dogs have a heightened sense of smell and hearing, they will also be supporting the night security to do the rounds and ensuring the property is safe and secure. [5]

ID cards for all staff members and visitors, staff members will have access to certain areas and data depending on their work or job title to be able to

carry out their daily duties this can be achieved through Role Based Access Control (RBAC), staff would need to be educated and trained in the security system that is in place so that employees know how to secure their system and part of the building that they access. Visitors ID passes would be given and depending on their reason for the visit would be restricted to those areas only with staff accompaniment. [5]

Fire detection and prevention measures would have to be in place to safeguard people and data information and equipment, and property damage. The proposal for the fire detection and fire prevention would be to ensure that the interior walls and doors are firewall, this would limit the spread if a fire were to occur. An automatic smoke and fire detection system. For the smoke detection system, the proposal would be for an air-aspiring detector for the server room, these detectors are ideal for high sensitivity areas as they are very sophisticated in detecting fires early through air-filtering and if smoke particles are detected through the laser system, the system becomes activated, this would safeguard all equipment within the server room. An ionization sensor for the rest of the building, these are also sophisticated systems which can detect fires early by detecting by-products when it enters the sensors chambers which then activates the detector. [5]

Steps that would be required to establish a secure information framework would be to have the following in place, policies and procedures and security implementations.

- A server room to centrally store and maintain all organisational data. This would enable the data and information security team to set up and manage the organisations network infrastructure.
- Security badges with limited access or a role base access to the server room. This would ensure only people that are meant to be there and have the right security credentials can access any area depending on their role or purpose, thus ensuring a better security defence against unwanted access to sensitive materials and data.
- Physical fire wall if possible, around the server room. This would reduce the damage impact on the server room and its equipment, as the server room would store all the organisations data.
- Fire detection and prevention system, to safeguard people, equipment and the building from fire damage, the proposed system is mention above.
- Intruder detection system. Would be detailed later in this paper.
- Security cameras, these are important part of security, as they can deter intruders as well as identify people who are accessing the building and its grounds. These would need to be monitored to ensure that early detection of any intruders or unwanted visitors are not accessing areas they are not meant to be.
- Set up network. This would involve starting with the basic of a firewall. A firewall is the barrier or gatekeeper of the security between your network devices

and the internet, it is a single point of defence between networks. A firewall will protect against threats such as malware and viruses. A firewall will scan incoming and outgoing network traffic for malicious content and filter it based on predetermined security rules, if it detects any threats or anomalies it will block it. We would then move onto setting up a VPN. [14]

- A Virtual Private Network (VPN) would create a secure network connection over the internet. A VPN will reduce the risks of cyber attacks through anonymity and encryption of the network connection. Through a VPN the IP addresses are hidden and only the VPN providers IP address is shown thus making it almost impossible for attackers to follow, identify and reach your own IP address. Through remote access using a VPN employees can remotely and securely access the organisations systems and data thus increasing the organisations employee productivity by giving them access to work from anywhere anytime, a VPN also provides secure file sharing through access control in its settings, this will allow through role-based access control to establish a hierarchical control of the file sharing and system access that each employee can have to ensure that employees can only gain access to, see and share what they should due to their role within the organisation. Once a VPN is correctly set up for use with the organisations restrictions it requires a low maintenance cost. [14]

- Set up role base access control (RBAC) this is to ensure that the organisation can control the limitations of what systems, data, files can be restricted, accessed by its employees and others who will be accessing the network. An employee's role will determine the level of access that would be granted by the organisation for that employee to be able to do their job. This can be achieved through the hierarchical access and constraints model of RBAC. This is set up and managed by the network administrators who will determine the access rights and privileges of all who will access the organisations network either on or off site based on job roles. RBAC will reduce information and data breaches due to the fact that employees will only have access to information and data needed to do the work within their role, reducing access to the more sensitive systems, information and data. [15] [16]
- Cryptography – Is the method of encrypting and decrypting email messages and plain text messages. Encryption is the method of encoding data to prevent it from unauthorized access, this is to ensure that data is transmitted securely within the network. The proposed system to be implemented and used would be the Advanced Encryption Standard (AES). AES uses block cipher called the Rijndael block cipher, a symmetric encryption advanced algorithm which uses 128, 192 and 256-bit encryption which is implemented in both hardware and software making it a robust

security encryption protocol. AES ensures network connections to be secure, private, and authenticated. It covers the CIA triad making sure the connection is confidential, available and integrity. [17]

- Physical security – will entail, security guards, guard dogs, security ID cards, fences, gates and walls around the perimeter, security cameras, smoke, and fire detection systems. These would help to secure the site from unwanted intruders.

Intrusion detection system.

An intrusion detection system (IDS) put in place would help the organisation to identify unauthorized intrusions and activities within the network. Any unwanted access to the network or its system would be an intrusion, those who gain access are looking for weaknesses within the system to be able to exploit it for access and to attack the network and its system. An intrusion detection system would secure the network framework and computer systems of the organisation against threats and malware, it would also detect, identify, and alert weaknesses and vulnerabilities within the system to the administrator. IDS's work like burglar alarms in the way that when it detects any forms of intrusion it raises an alarm in the forms of audible signals, email messages, popup windows or pager alerts. *“According to NIST SP 800-94, rev. 1, IDPS's use several different response techniques”* [5] [18]some of these are:

- IDPS's can modify its environment when it detects an intrusion by changing security configurations to disrupt an attack.
- Blocking access to the target systems or systems from the source of the attack.
- Blocking access to all targeted information assets.
- Terminating the user session or network connection over which the attack is being conducted. [5]

The primary purpose of an IDPS is to detect by early signs any intrusion and report it/raise the alarm letting the organisation act quickly to prevent or stop an attack but in the very least reduce the impact of the attack. An IDPS can detect a doorknob rattling and an attack reconnaissance, these are what is known as probing/testing the organisations network for vulnerabilities in preparation for an attack on the network system. This probing of the system gathers information about the organisation, its activities, and its assets, this is known as footprinting. An IDPS which can detect these activities early can alert administrators to prepare for an attack or minimise the damage from an attack. [5] [18]

Four primary IDPS technologies which are identified through the types of events they monitor and the way that they are deployed. These are Host Based IDPS, Network based IDPS, Wireless IDPS and Network Behaviour Analysis (NBA).

Host-Based IDPS (HIDPS) are used to determine when a system has been compromised and can warn administrators when anomalies, alterations,

deletions, or adjustments occur on the network, these are done through alerts and logs. IDPS's are usually installed on a server or a dedicated PC known as the host, these hosts continually monitor the characteristics of events occurring on a system. HIDPS's not only detect attacks but also when an attack occurs it monitors incoming and outgoing traffic. Areas a HIDPS monitors are system logs, network traffic, file accesses and modifications, running processes, changes to system configurations and application activities. Some of the limitations of HIDPS are that they are vulnerable to direct attack and attack to the host operating system, if this happens then the HIDPS would be compromised which leaves the network vulnerable, it can be vulnerable to Denial of Service (DoS) attacks, uses large amounts of host disk space and resources which can reduce system performances, cannot always detect multi host scanning which would leave it vulnerable to attacks that span multiple devices simultaneously on the network. [18] [5] [19]

Network-Based IDPS (NIDPS) are based on either hardware or software designed to monitor and analyse network traffic for intrusions. NIDPS agents/sensors can be deployed at different locations of the network to remotely monitor different segments of the network simultaneously to detect any intrusion or attacks, these will then report back to the central NIDPS which will then analyse the network traffic, look for suspected activities that it has been programmed to identify as a possible intrusion or attack. If the NIDPS detects any such information it will raise an alarm

and notify the administrator by means of notifications (email messages, text message, pop up windows). NIDPS looks for certain patterns in the network traffic to identify such attacks as DOS (Denial of Service) and PORT scan and many more but this would need setting up and programming the hardware to be able to detect or identify these threats or attacks. Some of the weaknesses of an NIDPS is that it can only monitor the network traffic in locations where the sensors are deployed leaving unmonitored locations vulnerable. NIDPS can get overwhelmed with the volume of network traffic and fail to recognize threats/attacks, they cannot analyse encrypted packets or fragmented packets, due to these factors an NIDPS can become unstable or stop working leaving the network vulnerable. [5] [19] [18]

Wireless NIDPS – These can be hardware or software based and provide enhanced security on the network. These systems are usually implemented to an existing WLAN infrastructure. Wireless IDPS's Monitors and analyses the traffic on a wireless network and are subject to a variety of threats. Wireless NIDPS works on layer 2 and 3 of the OSI model and evaluates remote traffic looking for intrusions and attacks such as man-in-the-middle, wormholes, spoofing, flooding, blackhole, and sinkhole. Wireless IDPS works with a centralised management station with sensors deployed in different locations, the sensors send information to the central station for an accumulated assessment for network intrusion. Some of the weakness of wireless IDPS are the

ranges of the sensors, atmospheric conditions, quality of the network card which can all affect the signals, distorted signals mean the messages sent will not be complete or sent at all leaving that area of the network vulnerable. They are unable to detect certain passive protocol attacks, this is when attackers scan the wireless network for the systems channel scanning scheme. [5] [19] [20]

Network Behaviour Analysis system (NBA) – These systems monitor the flow of network traffic to identify excessive packet flows which can show the signs that there could be an attack or that the hardware devices have a malfunction in the system. These systems most commonly detect attacks such as DoS, DDoS, scanning, worms, policy violations and unexpected application services, these are achieved through monitoring internal networks, packet checking, real-time blocking of malicious data and sites, and connections between internal and external networks. NBA systems work best when used in conjunction with other security tools and IDPS's. [5] [18] [19]

There are four possible states of IDP systems, a true positive is when the IDPS successfully detects a threat and raises the alarm, a true negative is when the IDPS detects activity but there is not any threat to the network or systems. These are good as they show that the IDPS is working and doing what it is built to do.

A false positive is when the IDPS mistakenly raises the alarm for normal or acceptable behaviour of the network, when there is not an

attack happening, a false alarm. If this happens frequently the administrators become insensitive to the alarms thus leaving the system vulnerable to actual attacks and intrusions. In real time this can be related to the story of the boy who cried wolf. [5] [19]

A false negative is when the IDPS does not react or detect when there is an intrusion or attack or accepts the intrusion or attack activities as acceptable. This is the most serious or dangerous state an IDPS can be as no one would be alerted that an attack is happening, and it cannot be stopped. This would show that the IDPS is not working or has been compromised through an attack. [5] [19]

The protection of an organisations assets is a fundamental part of security, a quality robust IDPS system to safeguard these assets is key to any security divisions. The proposed system would need to have the capabilities of detecting and preventing intrusion and attacks and be cost effective.

The proposed Intrusion detection and prevention system.

McAfee Network Security Platform (NSP). NSP is considered to be the next generation intrusion detection and prevention solution that protects systems and data wherever it is implemented, with features such as total protection supporting more than 30 million connections on a single device. NSP is flexible, simple with a comprehensive architecture using intelligent sensors to find and block sophisticated threats and intrusions. It also offers intelligent bot analytics, self- learning DoS

profiles, functions for identifying malicious hosts, flow data analysis, SSL decryption, behavioural analysis and learning engines, automation, and integration into endpoint security. NSP is a unified security defence management architecture which streamlines global threat intelligence with cloud and hybrid capability. It has a fast and accurate response to network threats. The architecture also featured with virtual SDN segments and is suited to hybrid cloud deployment. [21] [22]

Conclusion

It is evident that all modern-day organisations and its networks are prone to intrusion, cyber-attacks, and physical attack. The protection of the asset of the organisation is paramount to security. The main purpose of this assignment is to propose a security infrastructure that would meet the security needs of the organisation whilst at the same time meet government regulations related to information and data protection. This assignment identifies key roles and responsibilities that would be needed to ensure suitable assurances and governance of the organisation with respect to the information and data that would be stored and kept in accordance with the law. This assignment identifies some key policies and procedure that would need to be devised and implemented to meet government guidelines and information security laws and best practices. A suitable framework was suggested with examples of software's and hardware required to secure the organisations security including physical security, fire detection and prevention systems. The

assignment shows Steps that would be required to establish a secure information framework including the implementation and maintenance of security features and software's. another security feature that has been researched and presented in this assignment was an Intrusion Detection

System in network security. IDPS protect against internal as well as external intrusions and threats, it identified various IDS's their strengths and weaknesses and proposed a suitable IDPS security platform to meet the needs of the organisation.

Appendices

SANS Acceptable Use Policy

SANS Institute 2014 – All Rights Reserved Page 1 Consensus Policy Resource Community Acceptable Use Policy Free Use Disclaimer: This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org. Last Update Status: Updated June 2014 1. Overview Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to 's established culture of openness, trust and integrity. Infosec is committed to protecting 's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of . These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose The purpose of this policy is to outline the acceptable use of computer equipment at . These rules are in place to protect the employee and . Inappropriate use exposes to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by , the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with SANS Institute 2014 – All Rights Reserved Page 2 Consensus Policy Resource Community policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2 This policy applies to employees, contractors, consultants, temporaries, and other workers at , including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by .

4. Policy

4.1 General Use and Ownership

4.1.1 proprietary information stored on electronic and computing devices whether owned or leased by , the employee or a third party, remains the sole property of . You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

4.1.3 You may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.

4.1.6 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

SANS Institute 2014 – All Rights Reserved Page 3 Consensus Policy Resource Community

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the

device is unattended. 4.2.4 Postings by employees from a email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of , unless posting is in the course of business duties. 4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. 4.3 Unacceptable Use The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing -owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. 4.3.1 System and Network Activities The following activities are strictly prohibited, with no exceptions: 1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by . 2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which or the end user does not have an active license is strictly prohibited. 3. Accessing data, a server or an account for any purpose other than conducting business, even if you have authorized access, is prohibited. SANS Institute 2014 – All Rights Reserved Page 4 Consensus Policy Resource Community 4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question. 5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.). 6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. 7. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. 8. Making fraudulent offers of products, items, or services originating from any account. 9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties. 10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. 11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made. 12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty. 13. Circumventing user authentication or security of any host, network or account. 14. Introducing honeypots, honeynets, or similar technology on the network. 15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack). 16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet. 17. Providing information about, or lists of, employees to parties outside . SANS Institute 2014 – All Rights Reserved Page 5 Consensus Policy Resource Community 4.3.2 Email and Communication Activities When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department 1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). 2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages. 3. Unauthorized use,

or forging, of email header information. 4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies. 5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type. 6. Use of unsolicited email originating from within 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via 's network. 7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using 's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of 's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate 's policy, is not detrimental to 's best interests, and does not interfere with an employee's regular work duties. Blogging from 's systems is also subject to monitoring.
2. 's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by 's Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing SANS Institute 2014 – All Rights Reserved Page 6 Consensus Policy Resource Community comments when blogging or otherwise engaging in any conduct prohibited by 's Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of . Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, 's trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: <https://www.sans.org/security-resources/glossary-of-terms/>

- Blogging
- SANS Institute 2014 – All Rights Reserved Page 7 Consensus Policy Resource Community
- Honeypot
- Honeynet
- Proprietary Information
- Spam

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

[9]

SAN Email Policy

SANS Institute 2013 – All Rights Reserved Page 1 Consensus Policy Resource Community Email Policy

Free Use Disclaimer: This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.

Last Update Status: Updated

1 Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2 Purpose

The purpose of this email policy is to ensure the proper use of email system and make users aware of what deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Network.

3 Scope

This policy covers appropriate use of any email sent from a email address and applies to all employees, vendors, and agents operating on behalf of .

4 Policy

4.1 All use of email must be consistent

with policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. 4.2 email account should be used primarily for businessrelated purposes; personal communication is permitted on a limited basis, but non- related commercial uses are prohibited. 4.3 All data contained within an email message or an attachment must be secured according to the Data Protection Standard. 4.4 Email should be retained only if it qualifies as a business record. Email is a business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email. 4.5 Email that is identified as a business record shall be retained according to Record Retention Schedule.SANS Institute 2013 – All Rights Reserved Page 2 Consensus Policy Resource Community 4.6 The email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any employee should report the matter to their supervisor immediately. 4.7 Users are prohibited from automatically forwarding email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain confidential or above information. 4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct business, to create or memorialize any binding transactions, or to store or retain email on behalf of . Such communications and transactions should be conducted through proper channels using -approved documentation. 4.9 Using a reasonable amount of resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a email account is prohibited. 4.10 employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system. 4.11 may monitor messages without prior notice. is not obliged to monitor email messages. 5 Policy Compliance 5.1 Compliance Measurement The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. 5.2 Exceptions Any exception to the policy must be approved by the Infosec team in advance. 5.3 Non-Compliance An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. 6 Related Standards, Policies and Processes • Data Protection Standard SANS Institute 2013 – All Rights Reserved Page 3 Consensus Policy Resource Community 7 Definitions and Terms None. 8 Revision History Date of Change Responsible Summary of Change Dec 2013 SANS Policy Team Updated and converted to new format. [13]