Case Study: an Information Security Programme and Policies Implementation Proposal for North GenOne

Contents

Introduction

Background

North GenOne is an electricity generation firm that has recently been acquired by ReNewABC, a renewables company. North GenOne is a small business, with only 23 employees.

As part of the acquisition process, the current information security posture of the firm has been reviewed and several areas of concern have been highlighted. The assessment suggested that North GenOne is using outdated technology, weak or non-existent technical security controls and has a lack of existing information security policies or suitably trained staff. It was also noted that the company had recently fallen victim to a successful ransomware attack.

The directors of ReNewABC have expressed a desire that the staff at North GenOne are security aware, and that the firm become security compliant. They have requested that a proposal be written for North GenOne, outlining an appropriate information security program, and set of information security policies to be adopted.

Purpose

Recent research conducted into cyber breaches in the UK concluded that cyber security (and as a result, information security) has become less of a priority to smaller businesses due to the rising costs of implementing effective security controls (Department for Science, Innovation & Technology, 2023). It is important to ensure that the information security posture of any company being acquired (the Target) is of an acceptable standard to the acquiring company (the Acquirer) both during and after the acquisition process has been completed to reduce risk to the Acquirer (Sherer *et al*, 2015).

According to Mattord and Whitman (2017), information security performs four important functions for an organisation:

- Protecting an organisation's ability to function.
- Protecting any physical and electronic data that an organisation collects and uses.
- Enabling applications utilising the organisation's technology to function safely.
- Safeguarding the organisation's technology assets.

This report seeks to identify issues within North GenOne that pose a risk to these four important functions with a view to providing recommendations on what actions can be taken to reduce or eliminate the risk that they present. Any recommendations made will be supported with contextual information that will demonstrate the reasons a particular issue should be addressed. There will be a heavy reliance on the introduction of information security polices as these can provide a robust basis to the security posture of any organisation (The Cyber Express, 2023). A list of recommended policies will be provided in Appendix A. Further guidance will be given on how issues can be prioritised within the proposal.

Approach

Guidance on the implementation of an effective information security program will be taken from Whitman and Mattord (2019). Recommendations around a risk management framework implementation will be based upon NIST's 7-step RMF process (2018). Recommendations regarding controls will be made in line with the controls and objectives identified in Appendix A of ISO 27001 (Douglas Thornton Consulting, 2019) to ensure that the proposal contents are capable of fulfilling ReNewABC's desire for North GenOne to be compliant with a security standard, and to further support any recommendations made.

Proposal

There is an absence of policies and procedures with respect to risk management at North GenOne. As per NIST SP 800-37 Rev. 2 (2018), the area of risk management will be further divided to allow for the inclusion of targeted recommendations. NIST SP 800-37 Rev. 2 (2019) describes a 7-step approach to the implementation of a risk management framework:

1. Prepare.
2. Categorise.
3. Select.
4. Implement.
5. Assess.
6. Authorise.
7. Monitor.

Applying these steps to the findings of the review of North GenOne's information security posture identifies the following areas that this proposal will target with specific recommendations:

1. Asset Identification (Prepare/Categorise).
2. Risk Identification and analysis (Prepare/Categorise).
3. Vulnerability Identification (Categorise/Select).
4. Risk Treatment (Select/Implement/Assess).
5. Compliance and Monitoring (Authorise/Monitor).

Asset Identification

North GenOne have no official record of many of their assets, and thus have no way of understanding what vulnerabilities they possess, what risks those vulnerabilities present to the organisation, or what the consequences are of those risks being realised. As noted by Whitman and Mattord (2019), Tzu's observations around knowing your own weaknesses before being able to successfully defend them apply in this instance. North GenOne should begin work immediately to identify and document what their assets are. This will encompass all physical and logical assets, including hardware, software, network, data, and people assets. This process should also identify the individuals responsible per asset. These actions will correspond to the controls listed in section A8 of Appendix A of ISO 27001 (Douglas Thornton Consulting, 2019) for asset management.

It is noted that an Enterprise Resource Planning (ERP) system is currently being used at North GenOne for business and HR management. Whilst the information contained within this system may contribute to the formation of the asset register, it is recommended that all the information is reviewed for accuracy before it is committed to the register.

Control A8.1.3 of ISO 27001 specifies that the acceptable usage of assets should be defined at this stage. Whilst it has been recognised that an attempt to introduce an acceptable use policy (AUP) has previously failed owing to a lack of managerial support, the importance of such a document to ensure that the organisation avoids litigation or financial losses due to inappropriate employee behaviour cannot be ignored (Doherty *et al*, 2011). To avoid using language within the policy that might be considered too technical, a sample policy template has been provided for use in Appendix B (SANS, 2022).

Following the identification of any data assets in North GenOne's possession, consideration should also be given to the creation of a data classification system. Classifying data enables organisations to

understand the risk posed to them in the event of loss or theft of that data (De Groot, 2023). All existing data should then be categorised in accordance with this newly created labelling system.

Risk Identification and Analysis

As previously stated, there is a lack of a risk management framework within North GenOne. As argued by Humphreys (2008), effective risk management is crucial to the protection of an organisation's information assets. He further argues that the identification and analysis of the risks present is a critical step in implementing an effective defence against threats to the organisation.

In accordance with the guidance provided by Whitman and Mattord (2019), a value must be assigned to all information assets as they are identified. This value will assist in the formation of the identification and prioritisation of risks and represents the impact of any particular asset on aspects such as revenue, profitability, and public image of the organisation. North GenOne should look to carry out an impact assessment on each of its assets and assess the risks associated with those assets with a view to establishing a relative risk rating for each identified risk, which can be recorded in a risk register.

Vulnerability Identification

Whilst it is recognised that North GenOne had little formal documentation surrounding its information assets at the time of the review, there were several vulnerabilities described in some of the Target's critical infrastructure assets. The identification of existing vulnerabilities plays a crucial role in the risk management implementation process (Gartner, 2021). Once these vulnerabilities have been identified, work can progress to understanding how likely it is that those vulnerabilities can be exploited and what impact that would have on the Target and the Acquirer. North GenOne should use their newly created asset registers to identify any vulnerabilities that may be present within their organisation.

In addition to the general recommendations provided above, there were several specific vulnerabilities discovered during the initial review that should be investigated immediately:

- Outdated technology.
- Remotely accessible operational technology (OT).
- Lack of Bring-Your-Own-Device (BYOD) controls.
- Excessive privileged access rights.
- Human resource practices.
- Incident response planning.

Outdated Technology

During the information security program review, it was discovered that North GenOne are using a Windows Server 2012 Domain Controller (DC). This Operating System (OS) is now out-of-date, and no longer supported by Microsoft (i.e., security updates and patches are no longer being provided), putting the asset at a high risk of being exploited (Pagnotta, 2023). There is no secondary DC available should an incident occur, which would result in a complete shutdown of North GenOne's operations until the issue could be resolved. As a critical piece of North GenOne's infrastructure providing authentication and authorisation services to the entire business, this should be addressed as a matter of urgency (Compete 366, 2018). Given the lack of sufficiently trained staff (also discovered during the review), North GenOne may wish to consider outsourcing this service to an Infrastructure-as-a-Service provider. This would address the issues around redundancy and OS patching (Bhardwaj *et al*, 2010).

It was further discovered that there are several out-of-date endpoints (Windows XP and Windows 7) being used at North GenOne. Whilst it is appreciated that their existence may in part be tolerated due to the need to support legacy systems, both operating systems have been heavily targeted in recent years and the Target should investigate the possibility of upgrading these systems as soon as possible.

It is recommended that North GenOne develops a policy around the management of technical vulnerabilities, as well as a procedure for effective change management. These are outlined in controls A12.6.1 and A12.1.2 of Appendix A of ISO 27001 respectively.

Remotely Accessible OT

The review discovered that the OT at North GenOne, whilst being contained onsite, can be accessed remotely. It was also disclosed that the OT in use is outdated, though it is in the process of being updated. Given the criticality of OT to this organisation's operations, and the risk that unsecured and outdated OT can present to production and human safety (Peterson, 2023), the Target should examine the mechanisms in place for the remote access of these systems. Control A12.1.1 of Appendix A of ISO 27001 suggests that documentation of operation procedures in this instance would be beneficial. Peterson (2023) stipulates that consideration should be given to authorisation and authentication of users, security updates and patch management, as well as reviewing any encryption standards in place for data both at rest and in transit during remote connection sessions (or lack thereof).

Lack of Bring-Your-Own-Device (BYOD) Controls

During the initial review, it was reported that North GenOne does not currently implement any technical controls regarding access to its wireless network. Allowing non-company devices unfettered access to corporate resources creates problems around confidentiality and integrity of those resources due to potential security shortcomings on the device, as well as exposes the organisation to potential litigation and reputational damage should that device be stolen. Furthermore, any attempts to implement acceptable use policies around personal devices are often met with resistance (Keyes, 2013).

It is also possible that an attacker could use the unsecured wireless network to gain a foothold within the network, which could result in a successful attack against the organisation. In this instance, the consequences would be dependent on the attacker's objectives, but range from a simple website defacement to a complete shutdown of the business and theft or destruction of all corporate data (Positive Technologies, 2017).

North GenOne should examine the necessity of the BYOD capability in the workplace, considering the vulnerabilities that the current configuration creates within the corporate network. Control A6.2.1 of Appendix A of ISO 27001 can be utilised to mitigate or reduce the risks of unsecured devices accessing corporate resources.

Excessive Privilege Access Rights

The review examined the level of rights that users had to corporate resources. It was discovered that there is no current structure to the administrative rights given to users, and that most users have full rights to all data and systems. Furthermore, there is no access control policy in place that would provide guidance to system administrators on the appropriate use of access control. This lack of access control creates vulnerabilities around users gaining access to data that should not be available to them, causing issues with confidentiality and integrity of that data (Ng, 2013).

This unrestricted user access also provides an attacker with an easily achievable means to executing administrator-level commands should they gain access to the corporate network.

North GenOne should look to implement an access control policy following a review of existing access rights, removing or modifying access rights as necessary. A specific review of privileged access rights should be conducted as a minimum. These controls are outlined by controls A9.1.1, A9.2.5, A9.2.6, and A9.2.3 of Appendix A of ISO27001, respectively.

Human Resource Practices

North GenOne is a small family-run business. Many of its employees are relatives, and their staff turnover is low. Given this intimate nature of the firm, the policies surrounding onboarding and offboarding are non-existent, and most of the hiring and employment process is dependent on trust alone. Whilst this may result in a convivial working atmosphere, it has been recognised that the lack of security in these practices is a problem. A lack of pre-employment screening, appropriate use policies, or a suitable training program for employees creates opportunities for risks to be realised (Ulrich *et al*, 2021), as was evidenced with a successful ransomware attack against the company in previous months.

Work should commence on the creation of a screening procedure for new employees and a confidentiality or non-disclosure agreement as described in controls A7.1.1 and A13.2.4 of Appendix A of ISO 27001 respectively. Control A7.3.1 of the Appendix suggests documentation for the procedure following termination of employment or a change of responsibilities would be appropriate. North GenOne should also look to implement a training program for existing and future staff as per A7.2.3 of the appendix. Given the size of the Target organisation it may be beneficial to procure the services of an external training firm to ensure a high quality of training can be delivered (Kweon *et al*, 2021).

Incident Response Planning

Whilst not explicitly referred to during the information security review, the recent ransomware attack revealed that North GenOne has no documented incident response plan. According to IBM (2022), an effective incident response plan can significantly minimise the effects of an incident, reducing the damage and potential costs that can be incurred to an organisation.

North GenOne should look to include its lack of incident response plan as a vulnerability as part of the vulnerability identification process and initiate a program of work that will eventually satisfy all controls listed within sections A16 (Information security incident management) and A17 (Information security aspects of business continuity management) of Appendix A of ISO 27001.

Risk Treatment

During the initial review, it was identified that North GenOne has no planning measures in place for dealing with identified risk. Identifying an appropriate risk treatment plan for each Threat-Vulnerability-Asset (TVA) occurence allows an organisation to ensure that any residual risk remaining aligns with the organisation's risk tolerance. As the acquiring organisation, ReNewABC must be satisfied that there are no unacceptable levels of risk present prior to the full integration of the Target company (Deloitte, 2021). It has also been argued that the greatest benefit a risk treatment plan can provide is to ensure best value for a company's shareholders (Fatemi and Luft, 2002).

North GenOne should look to incorporate the findings of the previous phases of the information security program into thorough Business Impact Analysis (BIA) and Cost Benefit Analysis (CBA) documentation with a view to identifying which of the 5 basic risk treatment techniques (defence, transference, mitigation, acceptance, or termination) should be adopted for each TVA occurrence.

The outcome of the chosen risk treatment plan for each TVA occurrence should be documented within a risk register, and work can then commence on the implementation of any defence, transference, mitigation, or termination activities.

Compliance and Monitoring

Given the current lack of access controls and policies as has been discussed previously, North GenOne consequently has no measures in place to ensure compliance with those policies. Furthermore, there are no existing technical baselines that can be utilised to monitor compliance with technical controls or regulations. It is important for organisations to monitor compliance to baselines and policies to ensure that existing controls are in place and working in the way that they are intended (Diligent, 2022). Furthermore, an effective monitoring regime allows organisations to adjust any existing controls or policies to ensure that they remain effective (Alzahrani, 2023).

It is recommended that North GenOne develop a set of technical baselines that can be used to measure compliance. Furthermore, the controls identified in section A12.3 of Appendix A of ISO 27001 can be explored as measures to monitor the effectiveness of controls. North GenOne might also consider the implementation of a patch management programme to ensure that their systems are kept up to date. Looking to the future, it might be beneficial for the business to consider scheduling regular vulnerability assessments to ensure new and developing vulnerabilities are identified and remediated in an efficient manner (Whitman and Mattord, 2019), therefore maintaining system compliance.

Summary

When considering the outcomes of the initial review into North GenOne's current information security posture, it becomes clear that there are a number of important changes which need to be made before the risks posed to the Target's information assets can be considered reduced to a level acceptable to ReNewABC. This proposal has recommended a number of processes that North GenOne can follow that will allow the effective prioritisation of those risks and made suggestions on how the Target and Acquirer can collaborate to deliver a mutually agreeable treatment plan. It is envisaged that North GenOne will create a substantial amount of documentation during the implementation of the information security programme. A table of recommended policies and procedures, along with the corresponding controls from Appendix A of ISO 27001 (where applicable) has been provided in Appendix A of this document, separated according to each phase of the programme. Finally, suggestions have been made with regards to measures North GenOne can implement now that will ensure the compliance to their newly established policies and baselines for the future.

References

Alzahrani, A. (2023) 'Asset Identification Risk Management: Minimizing Risk, Maximizing Profit', *AMAN*, March Available at: https://www.aman.com.sa/blog/asset-identification-risk-management (Accessed: 12 November 2023).

Bhardwaj, S., Jain, L. and Jain, S. (2010) 'Cloud computing: A study of infrastructure as a service (IAAS)', *International Journal of engineering and information Technology*, 2(1), pp.60-63.

Compete 366, (2018) *Why a secondary DC is critical to operations*. Available at: https://www.compete366.com/blog-posts/domain-controller/ (Accessed: 12 November 2023).

De Groot, J., (2023) 'What is Data Classification? A Data Classification Definition', *DATAINSIDER Digital Guardian's Blog*, 5 September. Available at: https://www.digitalguardian.com/blog/what-data-classification-data-classification-definition (Accessed: 12 November 2023).

Deloitte (2021) *Identify key role of cybersecurity in Mergers and Acquisitions*. Available at: https://www2.deloitte.com/in/en/pages/risk/articles/role-of-cybersecurity-in-M-and-A.html (Accessed: 11 November 2023).

Department for Science, Innovation & Technology (2023) *Cyber security breaches survey 2023*. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023 (Accessed: 11 November 2023).

Diligent (2022) *What is compliance monitoring and why is it important?* Available at: https://www.diligent.com/resources/blog/the-importance-of-compliance-monitoring (Accessed: 12 November 2023).

Doherty, N.F., Anastasakis, L. and Fulford, H. (2011) 'Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy', *International journal of information management*, 31(3), pp.201-209.

Douglas Thornton Consulting (2019) *ISO 27001 Controls List*. Available at: https://www.douglasthornton.co.uk/wp-content/uploads/2019/11/DTC_Iso-27001-Controls-list-.pdf (Accessed: 11 November 2023).

Fatemi, A. and Luft, C. (2002) 'Corporate risk management: costs and benefits', *Global Finance Journal*, 13(1), pp.29-38.

Gartner (2021) *Vulnerability Management Should be Based on Risk*. Available at: https://www.gartner.com/smarterwithgartner/how-to-set-practical-time-frames-to-remedy-security-vulnerabilities (Accessed: 12 November 2023).

Gopalakrishnan, C. (2023*) Cybersecurity in Mergers and Acquisitions: The 10-point Checklist, The Cyber Express*. Available at: https://thecyberexpress.com/cybersecurity-in-mergers-and-acquisitions/ (Accessed: 11 November 2023).

Humphreys, E. (2008) 'Information security management standards: Compliance, governance and risk management', *Information Security Technical Report*, 13(4), pp.247-255. https://doi.org/10.1016/j.istr.2008.10.010.

IBM (2022), *What is incident response?*. Available at: https://www.ibm.com/topics/incident-response (Accessed: 12 November 2023).

Keyes, J. (2013) *Bring your own devices (BYOD) survival guide*. Boca Raton: CRC Press.

Kweon, E., Lee, H., Chai, S. and Yoo, K. (2021) 'The utility of information security training and education on cybersecurity incidents: An empirical evidence', *Information Systems Frontiers*, 23, pp.361-373.

NIST (2018) *NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (Accessed: 12 November 2023).

Ng, B.H. (2013) *Towards Least Privilege Principle: Limiting Unintended Accesses in Software Systems* (Doctoral dissertation).

Pagnotta, S. (2023) '5 Risks Of Outdated Software & Operating Systems', *BITSIGHT*, 19 September. Available at: https://www.bitsight.com/blog/outdated-software-issues(Accessed: 12 November 2023).

Peterson, E., (2023), *Achieving Visibility and Control in OT Systems: Remote Maintenance, Securing Remote Access, and the Zero-Trust Approach*. Available at: https://www.cisa.gov/sites/default/files/2023-05/Achieving%20Visibility%20and%20Control%20in%20OT%20Systems%20Remote%20Maintenace%2C%20Securing%20Remote%20Access%2C%20and%20the%20Zero-Trust%20Approach_508c.pdf (Accessed: 12 November 2023).

Positive Technologies, (2017), *Attacks on corporate Wi-Fi networks*. Available at: https://www.ptsecurity.com/ww-en/analytics/attacks-on-corporate-wi-fi-networks/ (Accessed: 12 November 2023).

SANS (2022), *Acceptable Use Policy*. Available at https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt1862b165519ffa1b/636f1a30bdef432fb152d0f8/Acceptable_Use_Policy.docx (Accessed 12 November 2023).

Sherer, J.A., Hoffman, T.M. and Ortiz, E.E. (2015). 'Merger and acquisition due diligence: a proposed framework to incorporate data privacy, information security, e-discovery, and information governance into due diligence practices', *Richmond Journal of Law & Technology*, 21(2), p.5.

Tzu, S. *The Art of War*. Translated by the Sonshi Group. Available at: https://www.sonshi.com/sun-tzu-art-of-war-translation-original.html (Accessed: 11 November 2023).

Ulrich, P., Frank, V. and Büttner, R. (2021). 'One Single Click is enough–an Empirical Study on Human Threats in Family Firm Cyber Security', *Proceedings of the 54th Hawaii International Conference on System Sciences | 2021*, pp. 4548-4556.

Whitman, M. E. and Mattord, H.J. (2019). *Management of information security.* 6th edn. Boston: Cengage Learning.

Whitman, M. E. and Mattord, H.J. (2018). *Principles of information security.* 6th edn. Boston: Cengage Learning.

Appendix A: Recommended documentation by programme phase and associated ISO 27001 controls

Phase	ISO 27001 Appendix A control(s) (if applicable)
Asset identification	
Asset inventory (including ownership details)	8.1.1 8.1.2
AUP policy (to include email and internet usage guidelines)	8.1.3
Data classification labelling structure	8.2.1 8.2.3
Risk identification and analysis	
Information asset impact worksheet	N/A
Threat analysis table	N/A
Vulnerability identification	
Management of technical vulnerabilities procedure	12.6.1
Change control management procedure	14.2.2
Operating procedures documentation	12.1.1
Mobile device policy	6.2.1
Access control policy	9.1.1 9.1.2 9.2.1 9.2.2 9.2.5 9.2.6 9.4.1 9.4.5
Privileged access management policy	9.2.3
Termination/change of responsibilities procedure	7.3
Screening procedure	7.1.1
Incident response plan. To include: * Disaster recovery plan. * Business continuity plan.	 16 (all) 17.1 (all)
Threats-Vulnerabilities-Assets (TVA) worksheet	N/A
Risk treatment planning	
Business impact analysis	N/A
Cost benefit analysis	N/A
Risk register	N/A
Compliance and monitoring	
Event logging policy	12.4.1
Backup policy (with regards to the protection of stored logs)	12.3 12.4.2
Patch management policy	12.6.1

Vulnerability management policy. To include: * Assessment schedule. * Procedures.	12.6.1

Appendix B: Acceptable Use Policy

SANS

Acceptable Use Policy

Last Update Status: *Updated October 2022*

1. Overview

Infosec Team's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. <Company Name> is committed to protecting <Company Name>'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, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company Name> 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 and other electronic devices at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct <Company Name> business or interact with internal networks and business systems, whether owned or leased by <Company Name>, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at <Company Name> and its subsidiaries are responsible for

exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with <Company Name> 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 <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

4. Policy

4.1 General Use and Ownership

4.1.1 <Company Name> proprietary information stored on electronic and computing devices whether owned or leased by <Company Name>, the employee or a third party, remains the sole property of <Company Name>. 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 <Company Name> proprietary information.

4.1.3 You may access, use or share <Company Name> 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 <Company Name> may monitor equipment, systems, and network traffic at any time, per Infosec's *Audit Policy*.

4.1.6 <Company Name> 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*.

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 lock screen 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 <Company Name> email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is during business duties.
4.2.5 Employees must use extreme caution when opening email 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 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 <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-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 <Company Name>.
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 <Company Name> 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 <Company Name> business, even if you have authorized access, is prohibited.
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, ransomware, etc.).

6. Revealing your account password/passphrase 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 <Company Name> 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 <Company Name> 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, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team 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 <Company Name> 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, <Company Name> employees to parties outside <Company Name>.

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, text, 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 <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'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 or posting to social media platforms by employees, whether using <Company Name>'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 <Company Name>'s systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>'s policy, is not detrimental to <Company Name>'s best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from <Company Name>'s systems is also subject to monitoring.
2. <Company Name>'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'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 <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by <Company Name>'s *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to <Company Name> 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 <Company Name>. 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, <Company Name>'s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging or social media 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
- Honeypot
- Honeynet
- Proprietary Information
- Spam
- Ransomware

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
Oct 2022	SANS Policy Team	Updated and converted to new format.