

**˗ˏˋ ☆ ˎˊ˗ |Star education| ˗ˏˋ ☆ ˎˊ˗**

Project 1-Part A



Nicole Kemp

April 4, 2023

Instructor: anar

Rmit

Cybersecurity, Cert IV  
Project 1-Part A

˗ˏˋ ☆ ˎˊ˗ |Star education| ˗ˏˋ ☆ ˎˊ˗

[Section 1: Information and security policies: 3](#_Toc131408493)

[A. Review each of Star education’s policies 3](#_Toc131408494)

[B. Outline the likely team members 3](#_Toc131408495)

[C. Suggest three (3) work habits 3](#_Toc131408496)

[D. Evaluate Star education’s configuration 3](#_Toc131408497)

[Section 2: Risk Assessment: 3](#_Toc131408498)

[A. Conduct an audit of Star education’s current security tools and infrastructure. 3](#_Toc131408499)

[B. Outline Star education’s baseline for their security infrastructure. 3](#_Toc131408500)

[C. Conduct a risk assessment on the organisation’s systems and human operations.. 3](#_Toc131408501)

[Section 3: Security vulnerabilities: 3](#_Toc131408502)

[a. Outline the security infrastructure vulnerabilities of the organization.. 3](#_Toc131408503)

[b. Provide a summary email 3](#_Toc131408504)

[**References:** 3](#_Toc131408505)

## Section 1: Information and security policies:

### Review each of Star education’s policies and note down at least three (3) implications of implementing these policies. Think about the effects on the students, staff, and the organisation itself.

|  |  |  |  |
| --- | --- | --- | --- |
| Policy: | Implication on Students | Implication on Staff | Implication on Organization |
| Acceptable  Use: | All Star education equipment, personnel, and resources are subject to this policy. | Star education employees and contractors are required to immediately report any suspected or actual violations of this policy. | Any violations of this policy may result in disciplinary action up to and including termination of employment or legal action. |
| Evidence: | * This policy applies to all users of Star Education's information resources and assets, including employees, contractors, consultants, temporary employees, and other workers.”(**Section 3.1**) * "Star Education's information resources and assets must not be used for any illegal or unethical purposes, including, but not limited to, unauthorized access, malicious damage, or unauthorized alteration of data." (**Section 3.3**) * "Star Education reserves the right to monitor, access, retrieve, read, copy, and disclose all information and data that is created, stored, accessed, transmitted, or received using its information resources and assets, including email, internet usage, and any other communication or data sharing system.” (**Section 4.2)** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Policy: | Implication on Students | Implication on Staff | Implication on Organization |
| Remote  Access: | Students can trust that their information is being accessed and handled securely, even when staff members are working remotely. | Staff members are required to ensure that their remote access connections are secure and compliant with the policy, which ensures that all network access is properly controlled and encrypted. | The policy ensures that Star education's corporate network is protected from unauthorized access and that all connections are secured, thus minimizing the potential exposure to damages that may result from unauthorized use of company resources. |
| Evidence: | * "This policy applies to all Star education employees, contractors, vendors and agents with a Star education-owned or personally-owned computer or workstation used to connect to the Star education network." - Implication on students: This means that any staff member who remotely accesses the Star education network must comply with the policy, ensuring that students' information is handled securely even when staff are working remotely.( **Scope section of the Acceptable Use Policy**) * "Authorized Users will not use Star education networks to access the Internet for outside business interests." - Implication on staff: This means that staff members are not allowed to use Star education networks for non-business related activities, which can help maintain network security and ensure that resources are being used for their intended purposes. (**Monitoring and Enforcement section**) * "An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment." - Implication on organization: This means that any violations of the remote access policy can result in serious consequences for the employee, up to and including termination of employment, which can help maintain compliance and minimize potential damages from unauthorized use of company resources. (Consequences **of Violations section.)** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Policy: | Implication on Students | Implication on Staff | Implication on Organization |
| Data  Breach: | Students' sensitive information is well-protected and safeguarded against any potential breach, ensuring their privacy and safety. | Staff members who handle sensitive information are held accountable and responsible for promptly reporting any security breaches, thus encouraging a culture of transparency and accountability. | By having a clear policy in place, Star education is able to minimize damages and quickly respond to any breaches, which can help maintain trust with students and stakeholders. |
| Evidence: | * "This policy mandates that any individual who suspects that a theft, breach or exposure of Star education Protected data or Star education Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@Stareducation.org, by calling 555-1212, or through the use of the help desk reporting web page at http://Star education.”(**section 1.1 Background.)** * "As soon as a theft, data breach or exposure containing Star education Protected data or Star education Sensitive data is identified, the process of removing all access to that resource will begin.” (**2.0 Scope)** * "The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources." (**Section 3.0 Policy Confirmed theft, data breach or exposure of Star education Protected data or Star education Sensitive data**) | | |

### Outline the likely team members who would be involved in reviewing these policies before they are implemented.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role: | Acronym: | Role Description: | | | Responsibilities: |
| CEO | Chief Executive Officer | Overall leadership and management of the company. | | | Providing guidance and approval for policies, ensuring they align with company strategy. |
| Responsibilities in a Crisis: | | | Leading the response to a crisis and communicating with stakeholders. | | |
| Responsibilities in Policy Review: | | | Providing guidance and approval for policies, ensuring they align with company strategy. | | |
| Role: | **Acronym:** | **Role Description:** | | **Responsibilities:** | |
| CIO | Chief Information Officer | Oversees information technology and systems within the company. | | Ensuring the integrity and security of company information systems. | |
| Responsibilities in a Crisis: | | | Coordinating the response to a crisis as it relates to IT systems. | | |
| Responsibilities in Policy Review: | | | Coordinating the response to a crisis as it relates to IT systems. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role: | Acronym: | Role Description: | | Responsibilities: |
| CFO | Chief Financial Officer | Oversees the financial operations of the company. | | Budgeting, financial planning, and risk management. |
| Responsibilities in a Crisis: | | | Assessing the financial impact of a crisis and managing financial resources. | |
| Responsibilities in Policy Review: | | | Assessing the financial impact of a crisis and managing financial resources. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role: | Acronym: | Role Description: | | Responsibilities: |
| CMO | Chief Marketing Officer | Oversees marketing and brand management for the company. | | Developing and executing marketing strategies. |
| Responsibilities in a Crisis: | | | Ensuring effective communication with stakeholders during a crisis. | |
| Responsibilities in Policy Review: | | | Ensuring effective communication with stakeholders during a crisis. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role: | Acronym: | Role Description: | | Responsibilities: |
| HR Director | Human Resources Director | Oversees the human resources function for the company. | | Recruitment, training and development, and employee relations. |
| Responsibilities in a Crisis: | | | Managing employee issues during a crisis and ensuring employee safety. | |
| Responsibilities in Policy Review: | | | Managing employee issues during a crisis and ensuring employee safety. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role: | Acronym: | Role Description: | | Responsibilities: |
| Legal Counsel | N/A | Provides legal advice and support to the company. | | Ensuring the company operates within legal requirements and manages legal risks. |
| Responsibilities in a Crisis: | | | Providing legal guidance during a crisis and managing legal risks. | |
| Responsibilities in Policy Review: | | | Providing legal guidance during a crisis and managing legal risks. | |
| Role: | **Acronym:** | **Role Description:** | | **Responsibilities:** |
| Department Managers | N/A | Oversees day-to-day operations of a specific department. | | Managing staff and operations within their department. |
| Responsibilities in a Crisis: | | | Coordinating response to a crisis within their department. | |
| Responsibilities in Policy Review: | | | Coordinating response to a crisis within their department. | |

### Suggest three (3) work habits that may impact on the successful implementation of the three (3) policies. For example, the staff members have been employed for a long time and therefore may be hesitant to update their passwords often. Provide a brief explanation as to why each work habit may impact on the policy implementation.

1. Lack of awareness: Insufficient training can result in a lack of awareness among staff members, leading to unintentional violations of security policies. As an example, if employees are not informed about the requirements for secure connections outlined in the Remote Access policy, they may connect to the network using unsecured devices or networks, thereby exposing sensitive information to potential security risks.
2. Resistance to change: If staff members are resistant to change, they may be hesitant to adopt new policies or procedures, which can hinder the successful implementation of the policies. For example, if employees are resistant to the Acceptable Use policy, they may continue to use company resources for personal purposes, which can impact the security and availability of those resources.
3. Lack of accountability: If staff members are not held accountable for their actions, they may be more likely to violate policies or engage in risky behaviour. For example, if employees are not held accountable for reporting security incidents or breaches, they may be less likely to do so, which can delay the response and resolution of those incidents.

### Evaluate Star education’s configuration within the organisation and outline the implications with regards to implementing cyber security policies. You will need to evaluate the organisation’s configuration against change management principles. This will include evaluating the following organisational information and reviewing how each of these areas are affected by change management.

Star education is a TAFE provider located in Melbourne that has recently reviewed its cyber security practices to ensure it is equipped to manage any cyber threats that may come its way. The Director is currently in a phase of revising many of the TAFE’s policies to ensure the safety of the TAFE’s students and staff. However, many staff members have worked at Star for a long time and may resist the implementation of new policies. Security training for staff is often incomplete, and students receive only basic security training during their first week at the TAFE. In addition, the organisation invests in some security tools, although these are at a basic level and are not always best suited to the growing size of the TAFE.

Star education's organisational structure includes:

* Academic operations
* Curriculum and teaching
* Student engagement and partnerships
* Corporate services,
* Strategy
* Performance and governance.

Each department has its own specific responsibilities, and any implementation of cyber security policies may need to be coordinated across departments to ensure effective implementation.

Change management principles should be applied to any implementation of cyber security policies, particularly given the potential resistance from long-standing staff members. The TAFE should consider:

* Involving staff members in the development and implementation of these policies to help build support for the changes.
* Invest in additional security training for staff and students to ensure they are equipped to handle any cyber threats.
* Reassess its security tools to ensure they are sufficient for its growing size and the potential cyber threats it may face.
* Consider how any implementation of cyber security policies may impact its overall organisational structure and processes, particularly given the involvement of multiple departments:

Job roles:

In order to make sure that the right people are in charge of dealing with cyber threats, job roles may need to be changed when cyber security policies are put into place. This will necessitate careful dialogue and discussion with staff members to ensure that any changes to their roles and responsibilities are fully understood. Furthermore, staff training will be required to ensure that they have the necessary skills and knowledge to effectively carry out their new roles.  
  
Student profiles:

Policies and procedures for dealing with cyber threats must take into account the various profiles of TAFE students, such as their age, level of technical expertise, and access to technology. The TAFE will need to tailor its approach to meet the needs of various groups of students, providing appropriate training and support to ensure that they are adequately prepared to manage cyber threats.

Management teams:

For cyber security policies to be put into place well, they will need strong leadership and management support. The management team must be fully engaged in the process, providing clear direction and guidance to employees, and ensuring that resources are appropriately allocated. Furthermore, regular monitoring and evaluation will be required to ensure that the policies are effective and achieve the desired outcomes.

Current systems that relate to cyber security:

The TAFE's current cyber security management systems will need to be thoroughly reviewed and evaluated to determine whether they are adequate to meet the growing threat of cyber-attacks. To do this, the hardware and software systems, as well as the network architecture and business processes that support these systems, will need to be reviewed. The security officer must collaborate closely with the relevant departments to identify any gaps or weaknesses in the current systems and devise a plan to address these issues. This could include upgrading hardware and software, instituting new policies and procedures, and providing additional training and support to employees.  
  
In sum the security officer needs to review the following areas of the organization:

-Organizational structure

-Hardware and software systems

-Network architecture

-Business processes

-Policies and procedures

-People (employees and contractors)

## Section 2: Risk Assessment:

### Conduct an audit of Star education’s current security tools and infrastructure. Provide at least one (1) example of the following types of tools:

|  |  |
| --- | --- |
| Tool Type | Examples |
| Packet sniffers and password auditing tools | Wireshark, Cain and Abel, John the Ripper |
| Penetration testing tools | Metasploit, Nmap, Nessus |
| Web vulnerability scanning tools | OpenVAS, Acunetix, Burp Suite |
| Encryption tools | VeraCrypt, GnuPG, BitLocker |
| Security hardware | Firewall appliances, intrusion detection and prevention systems, network switches with VLAN support |
| Network security monitoring tools | Security Information and Event Management (SIEM) systems, Snort, Suricata |
| Physical infrastructure tools | CCTV cameras, access control systems, biometric scanners |

### Outline Star education’s baseline for their security infrastructure. Think about the most essential components of the organisation that is their ‘heart and soul’ of security (i.e. key security elements). For example, there may be four (4) servers that provide/store/host the organisation’s most important data, thus these servers are the baseline that need to be secure as they can be.

Star education's baseline for security infrastructure includes the following key hardware and software components:

* Firewall: **Hardware** device could be a router with firewall capabilities like **Cisco routers** or **Ubiquiti routers**. Then using **Software** like **Cisco ASA** or **Fortinet FortiGate**, with updated policies and rulesets.

This hardware should be configured to allow authorized traffic in and out of the network, and its policies and rulesets should be updated regularly to reflect the latest security threats and best practices.

* Intrusion detection and prevention systems: **Hardware** Network interface card (NIC) like **Intel NICs** or **Broadcom NICs**. **Software** such as **Snort** or **Suricata**, with proper configurations and signatures.

This software should be configured to monitor network traffic for suspicious activity and should be updated regularly with the latest configurations and signatures to be effective against the latest threats. It should also alert administrators when potential security incidents occur. The NICs should have built-in instruction detection and prevention capabilities.

* Regular vulnerability assessments and patch management on **Hardware** like; servers, workstations, network devices, laptops, and pcs etc. They should be using **Software** like **Nessus** or **OpenVAS** that can do regular vulnerability assessments.

Staff must patch the system when any identified vulnerability has been discovered.

* Data encryption: **Hardware** external hard drives with hardware-based encryption, examples like **WD my Passport** or **Seagate Backup plus**. **Software**, such as **BitLocker** or **VeraCrypt**, on sensitive information and media (e.g., student records, financial data).

All media and sensitive information should be encrypted to prevent un-authorised access in the event of a security breach. Examples are including student records, financial data, and any other data that is deemed confidential or sensitive.

* Security awareness training program for employees and students - **Neither hardware nor software**.

All employees and students should receive awareness training to ensure they are aware of the best security practices. The program should cover password management, phishing awareness, user account management procedures, and other best practices. This should be created by the security officer, not an outside program. This is because its needs to be tailored to that company’s needs.

* Disaster recovery and business continuity planning: **Hardware**, external hard drives or USB flash drives for backups, Uninterruptible power supply (UPS) for power protection, spare laptops, or desktop computers for emergency use. **Software** solutions like **Veeam** or **Acronis** to back up data and ensure quick recovery in the event of a disaster.

Disaster recovery and business continuity plans should be in place to ensure that the organization can quickly recover from a security incident or other disaster. This includes regular data backups, emergency response procedures, and business continuity plans to ensure that critical operations can continue in the event of a disruption.  
  
In addition to the above devices, physical security measures like locks on servers and swipe cards on rooms can be implemented to keep computers and learning equipment safe.

* Locks on servers: All servers will be kept in secure rooms or cabinets with locks to prevent unauthorized access. Only staff members with appropriate permissions will be allowed to access these areas.
* Swipe cards on rooms: To further increase security, swipe card access will be implemented on all rooms containing computers and learning equipment. Only students, staff, and relevant maintenance personnel will be given swipe cards to access these areas.

### Conduct a risk assessment on the organisation’s systems and human operations. For this question, you will need to provide an extensive assessment that includes any part of risk to the company’s cyber security practices. You may present this information in a table format. When assessing the risks for human operations, ensure you provide details on the types of systems that are affected by human operations, e.g. students interact with emails and local server drives.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Company Asset | Key Stakeholders | Types of Threats | Likelihood of Incidents | Repercussions | Controls |
| Student records | Academic operations, IT | Cyber attacks, human error/malicious intent | 3 (high risk) | Data loss, legal action | Data encryption, access control, backups |
| Financial data | Finance, IT | Cyber attacks, human error/malicious intent | 2 (medium risk) | Data loss, fines and penalties | Data encryption, access control, backups, audit logs |
| Learning management system | Curriculum unit, IT | System failure, cyber attacks | 2 (medium risk) | Production downtime, data loss | Backups, disaster recovery plan, network segmentation |
| Network infrastructure | IT, network engineering | Cyber attacks, system failure | 3 (high risk) | Production downtime, data loss | Firewall appliances, intrusion detection and prevention systems, regular patch management |
| Email system | Corporate services, IT | Cyber attacks, human error/malicious intent | 1 (low risk) | Data loss, negative impact on company reputation | Access control, regular patch management, security awareness training |
| Physical assets (e.g. servers, switches) | IT, facilities | Natural disasters, system failure | 2 (medium risk) | Production downtime, data loss | Backup power, regular maintenance, disaster recovery plan |

**Heat Map:** The risk level is determined based on the likelihood and impact of a particular threat to a specific asset. The risk level is color-coded based on a traffic light system, with red indicating high risk, yellow indicating medium risk, and green indicating low risk. This heat map can help to prioritize which risks need to be addressed first and allocate resources accordingly.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Asset | Threat | Likelihood | Impact | Risk Level |
| Proprietary information | **Cyber attack** | **High** | **High** | **Red** |
| Hardware | **Natural disaster** | **Low** | **Medium** | **Yellow** |
| Software | **System failure** | **Medium** | **High** | **Red** |
| Client information | **Human error / malicious intent** | **High** | **High** | **Red** |
| Network topology | **Cyber attack** | **High** | **High** | **Red** |
| Email system | **Lack of resources** | **Medium** | **Medium** | **Yellow** |

## Section 3: Security vulnerabilities:

### Outline the security infrastructure vulnerabilities of the organization. For example, vulnerabilities are weaknesses in security that can expose assets to threats, e.g. untrained staff and students etc.

1. Untrained staff and students on security practices and policies.
2. Outdated hardware and software systems that lack security patches and updates.
3. Insufficient security controls and monitoring systems in place.
4. Lack of disaster recovery and business continuity planning.
5. Weaknesses in our network architecture.
6. Inadequate physical security measures, such as access control systems and CCTV cameras.
7. Lack of proper encryption and data protection measures.

### Provide a summary email which outlines these security vulnerabilities, addressing the email to the appropriate areas/management of the organization.

Subject: **Security Vulnerabilities at Star Education**

CC: Chief Information Security Officer, Director of IT,  
To: IT management

To Whom It May Concern,

In this email, I would like to draw your attention to some flaws in the current security infrastructure at Star Education. You are probably aware that the sophistication of cyber threats is growing, making it all the more important that we take preventative measures to safeguard our resources, employees, and students.

We have identified several vulnerabilities in our current security infrastructure that put the organisation at risk as a result of a comprehensive review. Among the vulnerabilities are the following:

Staff and students lacking security practices and policy education.

* obsolete hardware and software systems lacking security updates and patches.
* Lack of adequate security controls and monitoring systems.
* Lack of business continuity and disaster recovery planning.
* Imperfections in our network architecture.
* Insufficient physical security measures, including access control systems and CCTV cameras.
* insufficient encryption and data protection measures.

Cybercriminals can use these flaws to compromise our systems and steal or destroy sensitive information, causing us financial harm and possibly even irreparable harm to our reputation.

I therefore strongly advise that we take immediate action to address these vulnerabilities and bolster our security posture. This can be accomplished by:

1. Providing staff and students with regular security training and awareness sessions.
2. Updating our hardware and software to the most recent versions and implementing routine security updates.
3. Implementing robust access control and surveillance systems to detect and respond to potential security incidents.
4. Developing and testing business continuity and disaster recovery plans.
5. Regularly conducting security assessments and audits to identify and promptly address potential vulnerabilities.

Please do not dismiss this warning and help us put these suggestions into action to strengthen our security.

Furthermore, please do not hesitate to contact me if you require further information or have any questions.

Looking forward to hearing from you,

Nicole

**------------------------------------- end of Part 1 ---------------------------------**

# References:

*Cybersecurity Best Practices* (2022) *Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA*. Available at: https://www.us-cert.gov/ncas/tips (Accessed: April 3, 2023).

*Essential eight maturity model FAQ* (2019) *Essential Eight Maturity Model FAQ | Cyber.gov.au*. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained (Accessed: April 3, 2023).

*Information security manual (ISM)* (2021) *Information Security Manual (ISM) | Cyber.gov.au*. Available at: https://www.cyber.gov.au/acsc/view-all-content/ism (Accessed: April 3, 2023).

*Introduction* (2022) *OWASP Top 10:2021*. Available at: https://owasp.org/Top10/ (Accessed: April 3, 2023).

*SIFT®* (2022) *SANS Institute*. Available at: https://www.sans.org/resources/ (Accessed: April 3, 2023).

Stine, K.M., Quill, K. and Witte, G.A. (2017) *Framework for improving critical infrastructure cybersecurity*, *NIST*. Kevin M. Stine, Kim Quill, Gregory A. Witte. Available at: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity (Accessed: April 3, 2023).

*Strategies to mitigate cyber security incidents – mitigation details* (2018) *Strategies to Mitigate Cyber Security Incidents – Mitigation Details | Cyber.gov.au*. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents-mitigation-details (Accessed: April 3, 2023).