radcliffe

Information Security Policy

July 2023

Version history

Version Name	Date Amended	Summary of Changes	Status	Name
1.0	2023-07-06	Draft version creation	Draft	Ags Angelides
1.1	2024-02-29	Adjustments to antivirus policy	Final version	Ags Angelides

Contents

1. Introduction

This policy document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated, if necessary, by Management and IT department on an annual basis or when relevant to include newly developed security standards into the policy and distribute it to all employees and contracts as applicable.

2. Information security policy

Radcliffe Medical Media Ltd handles personal user and client information daily. Sensitive information must have adequate safeguards in place to protect them, to protect user and client privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Radcliffe Medical Media Ltd commits to respecting the privacy of all its users and clients and to protecting any data about users and clients from outside parties. To this end, the business is committed to maintaining a secure environment in which the user and client related data is handled.

Employees handling personally identifiable information and any other sensitive user and client data should ensure to:

- Handle said data in a manner that fits with its sensitivity
- Limit personal use of Radcliffe Medical Media Ltd information and work issued devices and ensure it does not interfere with your job performance
- Do not disclose employee information unless authorised
- Protect sensitive user and client data
- Keep passwords and accounts secure
- Request approval from the IT department prior to establishing any new software or hardware, third party connections, web applications, etc.
- Do not install unauthorised software on business issued devices unless you have approval from the IT team
- Always leave desks clear (both in the home office and in the business office) of any sensitive data and lock computer screens when unattended
- Information security incidents must be reported without a delay to the IT team.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed heiren, you should see advice and guidance from your line manager.

3. Acceptable use policy

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Radcliffe Medical Media Ltd established culture of openness, trust and integrity. Business is committed to protecting the employees, partners, clients, users and the Company itself from illegal and damaging actions by individuals, either knowingly or unknowingly.

3.1. Personal use of company issued devices

At Radcliffe Medical Media Ltd we recognise that our employees may occasionally need to use their business-issued devices for personal purposes. We believe in fostering a flexible work environment that respects the personal needs and work-life balance of our employees. However, it is important to maintain the security and integrity of our company data and resources. Therefore, we have established the following guidelines for acceptable personal use of business-issued devices.

1. **Limited and reasonable use.** Employees may use their business-issued devices for personal purposes. Personal use should be limited and reasonable, ensuring that it does not interfere with their job responsibilities or productivity.

2. **Exercise good judgment.** Employees are expected to exercise good judgment and adhere to the company's code of conduct when using their business-issued devices for personal purposes. This includes refraining from accessing inappropriate or unauthorised content, engaging in activities that may violate laws or regulations, or causing harm to the company's reputation.

3. **Privacy and confidentiality.** Employees must respect the privacy and confidentiality of company data and information. Personal use should not involve accessing, storing, or transmitting confidential or sensitive company information without proper authorisation. It is the employee's responsibility to ensure that personal use does not compromise the security or confidentiality of company data.

4. **Personal liability**. Employees are personally liable for any adverse consequences resulting from their personal use of business-issued devices. If any data loss, security breach or damage occurs to company resources or data during personal use, employees will be held accountable for any necessary remediation or recovery costs.

5. **Prohibited activities**. Certain activities are strictly prohibited on business-issued devices, whether for personal or work-related purposes. These include, but are not limited to, engaging in illegal activities, unauthorised sharing of confidential information, downloading or installing unapproved software, or accessing websites that pose security risks.

By adhering to these guidelines, employees can enjoy a certain level of personal flexibility while ensuring the security and productivity of our company. It is essential for all employees to understand and comply with this policy. Failure to do so may result in disciplinary action, up to and including termination of employment.

3.2. Opening emails securely

To maintain a secure computing environment and protect against potential threats, it is crucial for employees to exercise caution when opening email attachments and clicking on links. The following guidelines should be followed to ensure the safe handling of email attachments and mitigate the risk of phishing attacks.

1. **Verify the sender.** Before opening any email attachment or clicking on a link, verify the identity of the sender. Pay attention to the email address, display name, and any suspicious or unexpected requests. If the sender is unfamiliar or the email seems suspicious, refrain from opening attachments or clicking on links and report it to the appropriate IT department.

2. **Exercise caution with unexpected attachments and links.** Exercise caution when receiving unexpected email attachments or links, especially from unknown sources or from known sources where the attachment or link was unexpected. Cybercriminals often use email attachments and links as a means to distribute malware or launch phishing attacks. If in doubt, contact the sender through a separate communication channel to verify the authenticity and purpose of the attachment or link.

3. **Consider file types**. Be wary of certain file types, such as executable files (.exe), scripts, or macros, as they can be used to execute malicious code. Similarly, exercise caution with links that direct to suspicious or unknown websites.

4. **Avoid hover over links**. When encountering links in emails, avoid hovering over them with the cursor to preview the destination. Hovering can trigger unintended actions or reveal deceptive URLs. Instead, rely on other methods, such as inspecting the actual URL, to determine the legitimacy of the link.

5. **Keep software updated**. Ensure that all software, including email clients, web browsers, and applications used to open attachments or access links, are regularly updated with the latest security patches. Outdated software may contain vulnerabilities that can be exploited by attackers.

6. **Report suspicious emails**. If any email attachment or link appears suspicious, contains malicious content, or seems to be part of a phishing attempt, promptly report it to the IT department.

3.3. Security of company issued portable devices

Company-issued portable devices, such as laptops, tablets, smartphones, and other mobile devices, play a crucial role in supporting business operations. To ensure the security and protection of sensitive information and data, the following guidelines must be adhered to when using and safeguarding company-issued portable devices.

1. **User accountability**. Each employee is responsible for the security and proper use of the company-issued portable device assigned to them. Devices should not be shared with others unless explicitly authorised by the IT department.

2. **Reporting loss or theft**. Employees must immediately report any loss or theft of a company-issued portable device to the IT department and their manager and follow the organisation's procedures for reporting incidents.

3. **Device authentication**. All company-issued portable devices must be protected by strong authentication methods, such as PIN codes, passwords, biometric authentication, or passphrases. Laptops should be set to lock automatically after 15 minutes of inactivity.
   Please refer to Password Policy section on the password requirements.

4. **Software updates**. Employees must regularly update the operating systems, applications, and firmware on company-issued portable devices to ensure they have the latest security patches and protections against known vulnerabilities.

5. **Anti-malware protection**. Company-issued portable devices should have up to date anti-malware software installed to detect and prevent malicious software or applications from compromising the device or data.

6. **Physical security**. Employees should take appropriate measures to physically secure company-issued portable devices. This includes not leaving devices unattended in public places, locking devices when not in use, and storing devices in secure locations when not in use.

7. **Data backup**. Employees should regularly back up important data stored on company-issued portable devices to a secure and approved backup location or cloud service. This helps to mitigate the risk of data loss due to device damage, loss, or theft.

8. **Data transfer and sharing**. Data transferred or shared from company issued portable devices should be done through approved and secure methods, such as encrypted channels or authorised file-sharing platforms.

9. **Reporting security incidents**. Employees must report any suspected or actual security incidents involving company-issued portable devices promptly to the IT department. This includes incidents such as lost devices, unauthorised access, or suspected malware infections.
   Please see the Reporting Security Incidents Policy for more information.

10. **Cooperation in investigations**. Employees must cooperate fully with any investigations related to the security of company-issued portable devices, including providing necessary information, access to devices, or any other assistance required for incident response and forensic analysis.

3.4. Acceptable network locations

Public and similar locations pose specific security threats that need to be addressed. The following policies should be followed when using company-issued devices at network locations.

1. **Authorised networks**. Company-issued devices should primarily be used on authorised networks, such as the organization's internal network, home office network, or secured Wi-Fi networks specifically designated for business use.

2. **Guest or public networks**. Usage of company-issued devices on guest networks or public networks should be limited to essential business needs only and approached with caution. Employees should be aware of the increased security risks associated with these networks.

3. **Eavesdropping and network sniffing**. Public and similar locations, such as coffee shops, airports, and hotels, often have unsecured or poorly secured Wi-Fi networks. Attackers may attempt to eavesdrop on network traffic or use network sniffing tools to intercept sensitive information transmitted over these networks.

4. **Malicious hotspots**. Cybercriminals may set up fake Wi-Fi hotspots that mimic legitimate networks. Employees should exercise caution and verify the authenticity of Wi-Fi networks before connecting their company-issued devices.

5. **Shoulder surfing**. Public and similar locations often have a higher risk of shoulder surfing, where individuals attempt to gain unauthorised access to sensitive information by visually observing a user's screen or keyboard activities. Employees should be vigilant and take appropriate measures to protect sensitive information from prying eyes.

6. **Physical device theft**. The risk of physical device theft is higher in public and similar locations. Employees should ensure that company-issued devices are never left unattended and are stored securely when not in use.

7. **Two-factor authentication (2FA)**. Enable and use two-factor authentication for accessing any of the company resources. This adds an additional layer of security by requiring a second verification factor, such as a unique code sent to a mobile device, in addition to a password.

8. **Web browsing practices**. When accessing websites from public or similar locations, employees should be cautious and limit their interactions to trusted and reputable sites. Avoid entering sensitive information or credentials on unsecured or suspicious websites, such as those which do not use https.

3.5. Approved software

The use of pre-installed software on work-provided devices, such as laptops, is authorised. Certain role-specific software may be utilised by employees within their departments, and employees are required to seek approval from their respective line managers.

To acquire the list of currently approved software or seek approval for any additional software that employees wish to use, they must contact the IT department. The IT department will assess the proposed software to ensure alignment with the business's security requirements before granting approval for installation and use.

3.6. Approved web applications

Upon commencement of employment with the organisation, employees will be informed, based on their department, of the list of web applications essential for daily tasks by their respective line manager. These applications are officially approved for business use.

In the event that an employee desires to incorporate a new web application into their work or seeks information about the comprehensive list of approved business web applications and their respective owners, they must initiate a discussion with the IT team. The IT team will conduct a security assessment of the proposed application. If the application does not receive approval, employees are strictly prohibited from creating a new account within the said application using their business email address.

3.7. Use of WhatsApp and other messaging platforms

We recognise that the use of WhatsApp is often convenient and is used by our customers for that very reason. We therefore will allow our employees to use WhatsApp and other messaging platforms other than Teams, if they wish, but only when it is appropriate to do so.

However, there are a number of issues that must be considered when using WhatsApp and similar online messaging applications:

- WhatsApp is not designed to be used by businesses (unless business subscription is acquired), and as such does not provide any guarantees about its use in business scenarios. This means it is difficult for us to ensure any data (including contact data) is processed in accordance with UK GDPR or our security standards.

- Furthermore, there are various legal or business integrity reasons why it is not appropriate to use WhatsApp for discussion or exchange of information. Our existing processes and systems (e.g. email, Teams) are all in position because they help us manage the data we process including maintaining backups and other controls around communication, particularly with customers. For example, if you send an email or receive an email, the contents of the email are part of our backup facilities, where we back up the email servers – if the same conversation takes place via WhatsApp we have no ability to back up those conversations, so if a customer wishes to dispute an agreement, and it was no longer accessible via WhatsApp it would be difficult for us to prove the agreement with the customer.

The following sections therefore set out the circumstances where WhatsApp is appropriate and inappropriate for business communication.

Unacceptable use of WhatsApp

- When you need to discuss, distribute or process any categories of personal data as defined in UK data protection law. You should therefore not send any employee or customer personal data via WhatsApp, and you should not encourage others, including customers to do so.

- When you need to keep a record of a conversation (e.g. a customer agreement or transaction). In such situations you must follow usual company processes and make use of email and other documentary systems, as required.
- To contact a colleague or a customer if they have specifically asked you not to use WhatsApp.
- When WhatsApp is used:
  - In a way that, with reasonable likelihood, would result in a breach of data protection or privacy laws (e.g. GDPR).
  - To create or send any material considered to be offensive, obscene or indecent.
  - To create or send any material used to facilitate harassment, bullying or victimisation of anyone which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation.
  - To create or send any material with the intent of committing fraud or likely to deceive the recipient.
  - To create or send any material deemed illegal according to UK law including material which is defamatory, threatening, discriminatory, extremist or copyright infringing.
  - In a way that, with reasonable likelihood, would result in unnecessary use of the IT team's resources (e.g. that leads to a malware infection on a work device or our computer network).
  - In a way that, with reasonable likelihood, would result in disrupting the work of others or bring Radcliffe Group into disrepute.

Acceptable use of WhatsApp

It is acceptable for you to use WhatsApp (for work purposes) in the following, limited, situations:

- When a customer or colleague contacts you directly via WhatsApp, or indicates they are happy to be contacted via WhatsApp.
- Where contact does not involve the discussion or exchange of personal data – i.e. it should not be used to take customer details or to pass personal details of customers to another employee.

4. Access controls

Access controls are essential components of our information security framework, ensuring the confidentiality, integrity, and availability of our sensitive data and resources. The purpose of this section is to outline the guidelines and procedures related to access controls within our organisation.

Our access control objectives are as follows:

- **Confidentiality.** Limit access to authorised individuals or entities to prevent unauthorised disclosure of sensitive information.
- **Integrity.** Ensure that data and resources are not improperly modified, deleted, or altered by unauthorised individuals.
- **Availability.** Guarantee that authorised users have timely and uninterrupted access to necessary information and resources.

4.1. User authentication

- All users must authenticate themselves before gaining access to the organisation's systems and data.
- Multi-factor authentication (MFA) is mandatory accounts with elevated privileges and for any cloud based service. See Password Policy for more information.
- Strong password policies are enforced, requiring regular password changes and complexity standards.

4.2. Authorisation, privileges and access revocation

- Access privileges are granted based on job roles and responsibilities, following the principle of least privilege.
- Access requests must be submitted to and approved by the respective data owners or managers.
- Access rights are promptly revoked when no longer needed due to job role changes or project completion.
- Terminated employees' access is immediately revoked upon employment termination.

4.3. Administrative account request process

- The management and approval of Drupal, Azure DevOps, and other administrative accounts are exclusively handled by the in-house IT department. Individuals requesting such accounts must submit a written request to the IT team. The IT team will assess the necessity of the requested account and approve it if deemed necessary.
- AWS administrative accounts are managed and approved by the in-house IT department, and in certain instances, by the 3rd party Cloud Infrastructure consultancy (but not without the Radcliffe Group's knowledge or approval).
- All administrative accounts, including those not explicitly mentioned, must adhere to a password policy requiring a minimum length of 12 characters

with no maximum length restrictions, in cases where Multi-Factor Authentication (MFA) is not available.

- For accounts where MFA is available, the implementation of Multi-Factor Authentication is mandatory for all administrative accounts.

5. Password policy and device protection

To ensure the security of our systems and protect sensitive information, Radcliffe Medical Media Ltd has implemented a strong password policy in accordance with the Cyber Essentials guidance. Password strength and multi-factor authentication (MFA) settings are crucial aspects of our information security strategy.

5.1. Password strength

To enhance the strength of passwords and prevent unauthorised access, we have implemented the following guidelines. Only one of the options listed below needs to be met for non-cloud based services/systems:

- Use multi-factor authentication (MFA) in conjunction with a minimum password length of 8 characters where MFA is available.

- The password must be a minimum of 12 characters in length, with no maximum length restrictions, where MFA is not available.

Additionally, MFA must be applied to all Cloud Based services where it is being offered, including services such as Jira, Dropbox, MS 365, Marketo, AWS, Azzure, Survey Monkey, etc.

5.2. Compromised accounts

If you suspect your account may have been compromised or you notice anything suspicious whilst using your account, the account password must be changed instantly and the IT department must be notified.

The account should then be monitored for any other suspicious behaviour and any further observations must be reported to the IT department.

5.3. Default passwords

All default passwords must be updated before the devices or accounts are used.

5.4. Other password considerations

Do not reuse your passwords across different accounts.

You should never share your individual account passwords with anyone, including your colleagues.

Personal devices approved for business use must also follow specific password requirements. These are outlined in our Bring Your Own Device (BYOD) Policy.

5.5. Shared accounts and passwords

- Shared accounts should only be created when there is a legitimate business need. Each shared account must be justified and approved by the appropriate management personnel.
- Access to shared accounts should be limited to employees who require it to perform their job responsibilities. Unauthorised individuals should not be granted access to shared accounts.
- Each user accessing a shared account is individually responsible for maintaining the confidentiality and security of the account. They must not share the shared account credentials with others or use it for unauthorised purposes.
- Shared account passwords will be changed whenever there are personnel changes, including but not limited to employee termination and job position changes.
- The sharing of passwords for shared accounts should be done using secure methods, such as encrypted communication channels or password management systems that allow for controlled sharing.
- Every shared account must have an account owner who is responsible for managing the account and monitoring its usage. The account owner should regularly review and update access rights and remove access for employees who no longer require it.
- In the event of a security incident involving a shared account, please see the Incident Response section of this document.

5.6. Securing mobile devices and tablets

The following are the security requirements we have established to protect company issues mobile devices and tablets.

- In order to prevent unauthorised access, devices must be password protected using the features of the device in order to access the company network.
- Employees who wish to use their personal mobile phones and tablets to connect to the business network must comply with one of the following unlocking methods:
  - A 6-digit PIN code
  - A 6-character password
  - Biometric login

Note: Combining, for example, a 4-digit PIN and a biometric is now allowed, as it invalidates the security provided by the biometric login.

- Pattern passwords are not allowed on any devices approved for connecting to the company network.

5.7. Securing Windows laptops

Laptops running the Windows Operating System must meet the following device unlocking requirements:

- If the laptop is protected by a PIN code or device-specific password (not tied to a Microsoft account), the code or password must be 6 digits or characters long.
- If the laptop is protected by logging in to a Microsoft account, which is also used for other online services, the password must meet the following criteria:
  - A minimum length of 8 characters
  - No maximum length
  - Avoid using the same password elsewhere or selecting common, easily guessable passwords (e.g., dog's name, date of birth, birthplace, "password12345," etc.).
- If the laptop is protected by biometric login, it should either have no other login options or, if available, the PINs and passwords must adhere to the aforementioned rules.

5.8. Securing MacOS laptops

Laptops running on macOS mut be protected as follows:

- If the laptop is protected by a password or a passcode which is not linked to an Apple ID, then it must be at least 6 characters/digits long.
- If the laptop is protected by a password or a passcode which is linked to an Apple ID, then it must adhere to the following criteria:
  - A minimum length of 8 characters
  - No maximum length
  - Avoid using the same password elsewhere or selecting common, easily guessable passwords (e.g., dog's name, date of birth, birthplace, "password12345," etc.).
- If the laptop is protected by biometric login using Touch ID, it should either have no other login options or, if available, the PINs and passwords must adhere to the aforementioned rules.

5.9. Protection against brute force attacks on company issued devices

- Devices must implement measures to protect against brute-force attacks, such as one of the following:
- Throttling: Limiting the number of unsuccessful login attempts on the device, allowing a maximum of 10 guesses within 5 minutes.

- Locking: Automatically locking the device after 10 unsuccessful login attempts.
- If a device remains idle for five minutes, it must lock itself using previously mentioned methods.

6. Data protection and privacy

Please refer to our Data Protection Compliance Policy and Privacy Policy for further information.

7. Network security policy

The network security policy establishes the framework for safeguarding the integrity, confidentiality, and availability of our organization's network infrastructure and data.

- Our network architecture will be designed with security as a priority, implementing appropriate segmentation and isolation to limit the impact of potential breaches, including segregating our office wireless network from that of the visitors wireless network and separating our broadcast network from the rest.
- Only broadcast related devices will be permitted to connect to broadcast network via port forwarding rules which will be documented here. No wireless connections will be permitted on this network.
- There will be a firewall deployed to protect all three networks.
- Firewall admin panel will be accessible externally from outside the business network, however, it will be protected with a username and password which meets the business Password Policy. Access to the Admin panel will be restricted to the IT support team only.
- An option to connect to firewall externally to monitor it will also be provided to the employees within the business if necessary. This will be protected with a username and password which meet the business Password Policy.
- The AWS Web Application Firewall will be implemented to safeguard the cloud infrastructure powering our websites, by protecting us again DDoS, SQL Injection and cross site scripting attacks. The real time monitoring provided by this firewall allows us to identify and address any security issues promptly. Default AWS firewall rules will be implemented including up to date reputation lists.
- Network devices and infrastructure components will be regularly updated with security patches and firmware updates. Critical vulnerabilities will be addressed as a priority to minimise the risk of exploitation.

8. Patch management policy

The patch management policy outlines the procedures and guidelines for maintaining the security and stability of our organisation's software and systems by promptly applying patches and updates. This policy aims to mitigate vulnerabilities and reduce the risk of security breaches resulting from outdated software.

The primary objective of this policy is to ensure that all software, operating systems, applications and hardware components are consistently updated with the latest security patches and updates.

Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors.

In the event of zero-day vulnerabilities or critical security breaches, emergency patching will be performed to ensure rapid deployment without affecting operations. If the emergency patching is required on employee devices, all employees will be required to patch their devices on the same day.

Regular communication and awareness campaigns will inform users about the importance of patch management and encourage prompt installation of updates on their devices.

8.1. Security patching schedules

Drupal security patches will be applied once a month by the development team, as they become available.

Infrastructure (Linux and Bastion host) patches for Radcliffe Cardiology multi-site Drupal environment and Wordpress environment will be applied as follows:

1. Any critical patches will be applied within a month.
2. Any non-critical patches will be applied every 2 – 3 months.

Any website which runs on serviless compute engine AWS Fargate will be automatically patched when te updates become available (e.g. Radcliffe Medical Education).

For employee devices, including laptops and computers, operating system patches will be promptly applied upon release. Employees will be reminded to adhere to this practice during annual security training and subsequent security refresher training.

9. Anti-virus

- The primary objective of this policy is to safeguard the organsation's digital assets by preventing, detecting and mitigating the impact of malware through the use of antivirus solutions.

- Approved antivirus software will be selected based on its effectiveness, compatibility with our systems, ease of management and regular update frequency and it will be installed on all machines issued by the organisation, with no option for the end user to modify any of its settings.

- The antivirus will be automatically updated and it will provide real time protection each time a file is received, opened, downloaded, copied or modified. The antivirus will be able to protect against all types of latest viruses by having access to the latest antivirus definitions and signatures.

- Employees will be educated about safe online practices, avoiding suspicious links and downloads, and recognising potential malware threats. Regular awareness campaigns will remind users of the importance of following antivirus policies and procedures.

- Apple OS-based computers and laptops are exempt from the requirement of installing additional antivirus software. The built-in security tools, including Gatekeeper, Malware Removal Tool (RMT), and XProtect, are considered adequate for ensuring the security of these devices.

10. Incident response

The incident response section outlines our approach to identifying, responding to, and mitigating cybersecurity incidents, ensuring the swift recovery of normal operations and the preservation of sensitive information. This plan is aligned with the National Cyber Security Centre (NCSC) guidelines and serves as a framework for effectively managing security incidents.

10.1. Incident response steps

1. **Notify.** The person who had discovered the incident must notify the IT department as soon as the incident is found.

2. **Triage** (performed by IT department). Determine the incident severity. See section on Incident Severity. Critical and High severity incidents will be addressed as soon as they are discovered. Determine the incident type. See section on Incident Type. The type of the incident will determine the actions that follow.

3. **Communicate** (performed by the IT department). Critical and high severity incidents are to be communicated to everyone in the business, including any progress being made on its resolutions in a form of updates.

4. **Analyse, contain/mitigate, remediate/eradicate and recover** (coordinated by the IT department). Depending on the incident severity and type, it may be necessary to lower the impact of the incident first before fully stopping it. Once the incident has been eradicated, the data and systems will be recovered and returned to the 'business as usual' state. The entire incident analysis will be documented within a Jira ticket, Incident Log project.

Commented [AA1]: Are we happy to use Jira for this and have a separate project for all incident logs?

If so, we will need a new issue type with fields specific to incidents.

5. **Review and close down** (coordinated by the IT department). If future improvements are necessary to prevent similar incidents from happening again, these improvements will be documented to be implemented in the near future depending on the likelihood of the incident occurring again as determined by the analysis.

6. **Documentation** (carried out by the IT team). All the incidents will be documented using Jira Incident Log project, including the cause, severity, any other analysis, mitigation and remediation actions taken, recovery information and any future work planned, if necessary.

10.2. Incident severity

The matrix below defines the incident severity levels. Each incident will be addressed based on its severity level.

Severity	Definition	Examples
Critical	A critical incident that affects a large number of users in production. **To be addressed as soon as discovered.**	80% of employees unable to work. Critical systems offline (AWS Infrastructure, Drupal) with no known resolution. High risk to / definite breach of sensitive client or personal data. Severe reputational damage - likely to impact business long term.
High	A significant problem affecting a limited number of users in production or employees. **To be addressed as soon as discovered.**	50% of staff unable to work. Risk of breach of personal or sensitive data. Non critical systems affected or critical systems affected with known (quick) resolutions.
Medium	A minor problem that affects the service but doesn't have a serious impact on users. **The initial response to be conducted within a few hours. If the isolation of the affected systems is required, this should be completed within 24 hours. Investigation should be completed within a few days. Final resolution to follow the investigation results.**	Possible breach of small amounts of non-sensitive data. Low risk to reputation damage. Small number of non-critical systems affected with known resolutions.
Low	A low-level deficiency that causes minor problems. **The initial response to be conducted within a few days. Incident to be assessed and triaged within one week. Investigation to be completed within approximately 2 weeks. Final resolution to follow the investigation results.**	Minimal, if any, impact. One or two non-sensitive / non-critical machines affected. <10% of non critical staff affected temporarily (short term), e.g. phishing.

10.3. Incident type

Most common incident types are documented below, including their descriptions and the expected steps to be taken by the IT department.

Incident type	Description	Response
Malware	Malware is malicious software designed to infiltrate, damage, or gain unauthorised access to computer systems. It includes	Isolate the affected device from the network immediately. Report the incident to the IT team for analysis and remediation. Do not pay any

	viruses, worms, Trojans, ransomware, and spyware.	ransom demanded by ransomware.
Unauthorised access or intrusion	Unauthorised access occurs when an individual gains access to systems, networks, or data without proper authorisation.	Disconnect the compromised system from the network. Change passwords and credentials if necessary. Report the incident to IT and follow the incident reporting process.
Phishing and social engineering	Phishing involves fraudulent attempts to trick individuals into revealing sensitive information, often through deceptive emails, messages, or phone calls. Social engineering manipulates individuals into divulging confidential information.	Do not respond to suspicious emails or requests for personal information. Report phishing attempts immediately. If sensitive data was shared, report the incident to IT and follow the incident reporting process.
Data breach	A data breach involves unauthorised access or exposure of sensitive or confidential information, potentially resulting in data loss or leakage.	Contain the breach by isolating affected systems. Report the incident to IT and the Data Protection Officer (DPO). Follow data breach notification procedures as required by data protection laws.
Denial of Service (DoS) or Distributed Denial of Service (DDoS) Attacks	DoS attacks disrupt services or networks by overwhelming them with excessive traffic. DDoS attacks involve multiple compromised systems targeting the same service.	Activate DoS/DDoS mitigation measures if available. Report the incident to IT and external network service providers if necessary.

10.4. Key contacts

The IT department should be contacted as soon as the incident is discovered to ensure it can be addressed in the timely manner:

- Wells Powell – CTO - wells@reddishgreen.co.uk
- Luke Donnebaum – IT Programme Manager - luke.donnebaum@radcliffe-group.com
- Ags Angelides – Technical Project Manager – agne.angelides@radcliffe-group.com

11. Employee awareness and training

Employee awareness and training are critical components of our information security strategy. This section outlines our commitment to educating employees about cybersecurity best practices, promoting a security-conscious culture, and ensuring that all staff members understand their roles and responsibilities in maintaining the security of our organisation's information and assets.

- Annual security training will be conducted to educate employees about various security risks, including phishing, social engineering, malware and data breaches.
- Awareness training will cover both general security topics and the specific security aspects relevant to the organisation. Employees will be trained on secure IT practices, including strong password management, safe browsing, secure file handling, and regular software updates. Use of personal devices for work-related tasks will also be covered to prevent security risks.
- All new employees will be provided with the security training during the onboarding process.
- The refresher training will be carried out at least twice a year which will discuss the latest security developments and will assess employee knowledge and understanding in situational quizzes.
- The effectiveness of security training programs will be regularly evaluated through assessments and feedback from employees. Training materials will be updated based on emerging threats and feedback.

12. Physical security

The Physical Security policy encompasses measures and controls designed to protect the physical assets, facilities, and resources that house and support our information systems, as well as the remote work environments of our employees. The primary goals of our combined physical and remote security policy are:

- **Prevent unauthorised access.** Physical access controls are maintained for our offices. For remote work, employees are required to implement robust authentication mechanisms, including strong passwords and multi-factor authentication (MFA), to prevent unauthorised access to our systems and data.
- **Protect equipment and assets.** Security measures to safeguard office equipment and hardware remain in place. For remote employees, when not using the work equipment, store your laptop and other devices in a secure location. If you live in a shared accommodation, lock the room or use a lockable drawer for your equipment.
- **Ensure business continuity.** Our physical facilities and remote work setups are designed to ensure the continuity of operations. This includes redundant power supplies for office network and broadcast equipment. Remote workers should ensure their devices are always fully charged, in case of power interruption and that the data is always backed up.
- **Visitor management.** In physical offices, visitor protocols remain in place. For remote work, employees are reminded to maintain the security of their home offices and avoid unauthorised access by family members or visitors. Please see Visitor protocol section for more information.
- **Data disposal.** Secure disposal of physical media remains a priority, and guidelines for remote employees are provided for the secure disposal or sanitisation of data-bearing devices within the **Clear desk audits** section.

- **Employee training.** All employees will receive training in physical and remote security best practices, including securing their remote work environments and identifying phishing attempts.

12.1. Clear desk and clear screen audits

Clear desk and clear screen audits are regular assessments conducted to ensure that employees maintain clean and secure workspaces. These audits help us to mitigate risks of unauthorised access to sensitive data, it ensures our compliance with laws, industry regulations and internal policies and it promotes secure culture among our employees.

Process for keeping desks clear

1. Always lock your computer or mobile device when leaving your workspace, even for short breaks. Use strong passwords or PINs for authentication. See our policies on stron passwords and PINs.
2. Store physical documents containing sensitive information in locked filing cabinets or drawers when not in use. Do not leave them on your desk or in unsecured areas.
3. Dispose of any documents that are no longer required by shredding them. Do not simply throw them in the trash.
4. Keep USB drives and other removable media containing sensitive data in a secure location when not in use. Do not leave them connected to your computer.
5. Ensure that all drawers and cabinets containing sensitive materials are locked when you step away from your desk.
6. At the end of each workday or when you leave your workspace, remove all papers, documents, and personal items from your desk. Leave only essential items on your desk.
7. If you notice any unauthorised individuals near your desk or suspicious activity, report it immediately to your manager and the IT team.

Compliance and consequences

Random clean desk audits will be conducted on quarterly basis. Any issues will be flagged up to the managements and additional training will be provided to the non-compliant employees.

Repeat non-compliance with the clear desk policy and security procedures may result in disciplinary action. It is essential for all employees to take personal responsibility for maintaining a secure work environment and protecting sensitive information.

Clean desk audit template

Clead desk audits will be carried out following the template provided by the IT department which can be found in SharePoint and accessed using the link below.

https://radcliffecardiology.sharepoint.com/:x:/s/RadcliffeIT/EUk7qLBseAFBjJ8faAjNSm8BI39xO-_MFaVDcSWjBLCECg?e=rze8lh

The template will be reviewed annually or more often, if the business needs or the regulations change.

12.2. Remote work guidelines for desk and device security

While remote workers may not be subject to clear desk audits conducted in physical office spaces, it is crucial for them to adhere to security guidelines that apply to maintaining a clear and secure workspace in their remote environments.

1. Just as in the office, remote workers should lock their computers and mobile devices when not in use, even in their home offices. Use strong passwords, PINs, or biometric authentication methods to secure access. Please see our strong password and PIN policies.
2. Store physical documents containing sensitive information in locked drawers or cabinets in your home office when they are not needed for work. Avoid leaving them on your desk or in unsecured areas of your home.
3. Dispose of physical documents that are no longer necessary by shredding them. Do not throw sensitive documents in the regular trash.
4. Keep USB drives and other removable media containing sensitive data in a secure location, such as a locked drawer, when not actively using them. Disconnect them from your computer when not needed.
5. At the end of each workday, clear your remote workspace of papers, documents, and personal items. Leave only essential work-related items on your desk or designated workspace.
6. Ensure that your home Wi-Fi network is secure with a strong password and WPA3 encryption. If you do not know how to secure your home network, please contact your IT team.
7. Promptly report any security incidents or concerns to your manager and the IT team. This includes any unauthorised access, suspicious activity, or potential data breaches.
8. Stay informed about security best practices for remote work and attend training sessions provided by the organisation to enhance your awareness and knowledge of security protocols.

12.3. Visitor protocol

1. **Scheduled visits.** Visitors should be scheduled in advance whenever possible. Visitors must notify host employees in advance of expected visit, providing their name(s) and expected arrival times.
2. **Check-in**. Upon arrival, visitors must be greeted by the host employees. The access codes to the building must not be shared.
3. **Escort requirement.** Visitors must be escorted at all times by an authorised host employee while in the office. The host is responsible for ensuring that visitors adhere to security policies.
4. **Wifi.** Visitors are only permitted to connect to our guest wifi, when necessary.

5. **No photography or recording.** Photography, audio, or video recording within the office premises is strictly prohibited without prior authorisation.
6. **Check-out.** Upon leaving, visitors must be escorted to the exit by the host employee.
7. **Emergency evacuation.** In the event of an emergency or evacuation, host employees are responsible for ensuring that their visitors safely exit the building through designated evacuation routes.

13. Vendor and third party security

Our organisation recognises the importance of maintaining the security and privacy of our systems and data when engaging with vendors and third-party providers. To ensure compliance with the UK General Data Protection Regulation (UK GDPR) and National Cyber Security Centre (NCSC) guidelines, we have established the following guidelines for assessing and managing the security of these partners.

Vendor assessment and selection

1. Before engaging with a vendor or third-party provider, conduct a comprehensive risk assessment to evaluate the security risks associated with their services or products.
2. Consider the vendor's security practices, compliance with industry standards, and their ability to protect the confidentiality, integrity, and availability of our data.
3. Assess their incident response and breach notification capabilities, as well as their data handling and retention policies.

Due diligence

1. Perform background checks, where applicable, on potential vendors, including their financial stability, reputation, and previous security incidents or breaches.
2. Evaluate their compliance with regulatory requirements, such as UK GDPR, as applicable to their services.

Vendor security standards

Establish security standards and requirements that vendors must adhere to when handling our data or accessing our systems. These standards should align with UK GDPR and NCSC guidelines. Alternatively, confirm the security standards discussed in the contract, are suitable and provide enough security.

Contractual agreements

1. Include specific security clauses and obligations in contracts with vendor, where possible. These clauses should detail their responsibilities for data protection, incident reporting, and compliance with our security policies.
2. Define the scope of services, data handling requirements, and expectations for security audits or assessments.

Data Protection Impact Assessments (DPIAs)

Conduct DPIAs when engaging with vendors who may process personal data on our behalf. These assessments should evaluate the potential impact on data subjects and the necessary safeguards to mitigate risks.

Termination and exit strategy

1. Include provisions in contracts that outline the process for terminating the relationship with vendors, including data handover, secure data disposal, and the return of assets.
2. Ensure that terminated vendors no longer have access to our systems or data.

Compliance verification

Ensure that vendors are aligned with any changes in security standards or regulations.

14. Compliance and legal requirements

Our organisation is fully committed to upholding the highest standards of information security and complying with all relevant laws, regulations, industry standards, and contractual obligations within the territories where we conduct our business.

We will adhere to all applicable laws and regulations governing information security and data protection. This includes but is not limited to:

- **UK General Data Protection Regulation (UK GDPR).** We will ensure the lawful and transparent processing of personal data, respect individuals' rights, and maintain records of data processing activities.
- **Data Protection Act 2018.** We will comply with the provisions of the Data Protection Act 2018, which supplements and extends data protection laws in the UK.
- **Network and Information Systems (NIS) Regulations.** We will meet the requirements of the NIS Regulations, ensuring the security of our network and information systems.
- **Cyber Essentials.** We will follow the Cyber Essentials framework where possible to protect against common cyber threats and ensure the security of our IT systems.

We are also committed to fulfilling all contractual obligations related to information security and data protection, whether with customers, partners, or third-party service providers. We will incorporate necessary security provisions into contracts and agreements, ensuring that all parties understand and meet their respective obligations.

15. Policy enforcement and review

Our organisation is dedicated to the effective enforcement of this information security policy. Policy compliance will be regularly monitored, and employees are expected to adhere to its provisions. Periodic reviews will be conducted to ensure that the policy remains relevant and aligned with evolving security needs and regulatory requirements. Any necessary updates or modifications will be made in accordance with best practices and industry standards. Violations of this policy may result in disciplinary action.

16. Approval

Name	
Signature	
Approval Date	
Review Date	