RIVERROCK

May 2022

IT Infrastructure,

Data and Information Security Framework

Document control	
Document Title	IT Infrastructure, Data, and Information Security Framework
Version	V8
Supersedes	Information Security Policy & Telecommunications Policy v7 & Cybersecurity awareness & prevention v3
Previous Review Date	May/2019
Version Approval Date	
Approved by	Exec Com
Ownership	Head of IT

Table of Contents

Glossary 6
Introduction 7
Policy Statement 7
Scope 8
Requirements & Guidelines 8
Network Security 8
Physical Security 9
Computer Security 9
File Storage and Naming Convention 9
Printing 9
Data Destruction Policy 9
Screen Locking 9
Memory Sticks and Removable Media 9
Mobile Devices 10
Leaving RR Or Moving into Another Role 10
Passwords and Accounts 10
Backups 11
Network Shared Drives 11
Viruses 11
Network Accounts 11
Clean Desk Policy 12
Internet 12
Provision 12
Downloading of Information Resources 12
Uploading Data/Information to The Internet 13
Prohibited Activities 13
Internet Filtering and Blocking 13
Internet Chat Facilities and Social Networking 13
E-mail 14
Metadata 14
Definition 14
Removing Metadata 14
Cyber Security 15
Cyber-Attack 15
Different Types of Cyber-Attacks 15

Methods to Prevent Cyber-Attacks 17
How to Deal with a Cyber-Attack 18
IT Infrastructure, Data & Information Security Risk Assessment 18
Unacceptable Behaviour 20
Remote Working 20
Incident Reporting 21
Management of User Accounts: Leavers 21
User's Responsibilities 21
Manager's Responsibilities 22
Appendices 23
Appendix 1: Use of Email and Calendar 23
Appendix 2: References 25
Annexure A: 26

Glossary

Authorized user - Authorized users are people acting within the scope of a legitimate affiliation with the university, using their assigned and approved credentials (ex. network IDs, passwords, or other access codes) and privileges, to gain approved access to university information technology resources.

Unauthorized user - A person acting outside of a legitimate affiliation with the university or outside the scope of their approved access to university information technology resources is considered an unauthorized user.

Breach - The acquisition, access, use, or disclosure of information in a manner not permitted under existing law which compromises the security or privacy of the information (i.e., poses a significant risk of financial, reputational, or other harm to the individual and/or university).

Confidentiality - Considers the effects of the inappropriate disclosure of the information.

Data - Data are symbols or characters that represent raw facts or figures and form the basis of information.

Critical data - Data that is essential for success, or data that must be retained for regulatory purposes. Typical examples of critical data include Customer data, especially personal information that is covered by data-protection laws. Employee data. Data concerning vendors and business partners.

Personal data - also known as personal information or personally identifiable information, is any information related to an identifiable person.

Encryption - Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to conceal the data's original meaning to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Firewall - A system designed to prevent unauthorized access to or from a private network.

Information - Data that has been given value through analysis, interpretation, or compilation in a meaningful form.

Information system - A discrete set of information resources, procedures and/or techniques, organized or designed, for the classification, collection, accessing, use, processing, manipulation, maintenance, storage, retention, retrieval, display, sharing, disclosure, dissemination, transmission, or disposal of information. An information system can be as simple as a paper-based filing system or as complicated as a tiered electronic system.

Privacy - The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

Security incident - A security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Security incident also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, misrouting of mail, or compromise of physical security, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.

Introduction

This document sets out RiverRock European Capital Partners LLP, all subsidiaries, appointed representatives, and related companies (together "**RiverRock**", "**RR**", the "**Company**" or the "**Firm**") information security policies and procedures and the responsibilities of everyone using RR systems and IT. Information security is of paramount importance to the Company to protect confidential and vulnerable data, ensure compliance with legislation and demonstrate that the Firm understands and applies best practices and processes to protect IT infrastructure, data, and information at all levels.

This Framework establishes the following principles to protect the infrastructure and Company information:

- All staff should ensure proper use, maintenance, and protection of all IT infrastructure they use or otherwise have access to
- Access rights should be allocated and revoked on a "need basis" and with management approval.
- All staff should consider the sensitivity of the information they handle, in whatever form, and protect the same by following the requirements and guidelines provided in this Framework.
- Line management must ensure these policies are duly circulated, implemented, and monitored at all levels
- Any breach of the outlined policy must be notified to the IT department at the earliest possible. Any such breach may result in disciplinary action in accordance with the Company's disciplinary procedures or, in the case of users who are not employees, may be considered a breach of the terms of any agreement by which such user is directly or indirectly permitted to use RiverRock's systems.

Any breaches of security (and non-compliance with this Policy) must be reported to the IT Manager and the COO (Chief Operating Officer) at the earliest possible. This is to safeguard the company and limit potential damage from information loss. RiverRock reserves the right to suspend or cancel any user's access to its systems in case of a suspected or proven breach of this policy or when RiverRock, in its absolute discretion, may consider appropriate to protect the integrity of its systems and the confidentiality of its information.

This Framework shall be reviewed annually, or whenever there is significant event or change in the IT infrastructure.

Policy Statement

It is the policy of RiverRock to ensure that all IT infrastructure, information systems, data and information developed, used, and/or stored by RiverRock are secure and comply with the requirements of the Data Protection Act 1988, the Computer Misuse Act 1990 (as amended) and the expectations of the Financial Conduct Authority.

Security policies at RiverRock are broadly based on three critical principles:

- Confidentiality
- Integrity

- Availability

The policies ensure that:

- Systems and information are protected against unauthorised access
- Measures to maintain information confidentiality are in place
- The integrity of information is maintained by protection from unauthorised modification
- Regulatory and legislative requirements are met
- Contingency plans are produced and tested as far as is practicable to ensure business continuity is maintained
- Information security training is provided for all staff
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action taken
- Sharing of information with other organisations/agencies is permitted under due approval and within the remit of a formally agreed information sharing protocol.

Scope

All RiverRock staff and third parties with access to RiverRock equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Company's equipment and the information that they use or manipulate.

All staff must be fully aware of the need to maintain secure systems and fully understand their responsibilities as outlined in this document. All staff are responsible for ensuring that they understand and abide by the policy. Failure to do so may warrant disciplinary action against the responsible party.

Where services are provided to the Company by outside organisations, it shall be ensured that the provisions of this policy are known to and accepted by that organisation as part of the contract.

Requirements & Guidelines

Information security is not just a matter of restricting unauthorised access to data; it is also a question of ensuring that the confidentiality, integrity, and availability of the data is maintained. This applies equally to IT systems and paper files. This Framework sets out the minimum requirements and guidelines that are to be followed by all and everyone with access to and/or rights to use, process and retain data/information:

Network Security

Non-RiverRock owned equipment must not be connected to or installed onto the Company's data network, communications facilities or any RiverRock owned computer under any circumstances without the written consent of the IT Head. The Company provides a publicly available wireless network which is secure and separate from the Company's business network for guests.

Physical Security

Access to RR equipment, systems, data, and information (held on information systems and in paper format) should be managed by ensuring appropriate security measures are in place in all RR offices and buildings where data is held. The buildings must have appropriate control mechanisms in place for the type of information and equipment that is stored there. Identification and access tools (e.g., badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned or provided to anyone else.

Visitors should be always escorted when entering secure areas and staff working in secure areas should challenge anyone not wearing an identification badge/visitor's pass who is unaccompanied.

Computer Security

All staff are responsible for data entered onto RR computers and have legal responsibilities under the Data Protection Act and the Computer Misuse Act to ensure that unauthorised access (including to other staff within RR) is prevented. All concerned staff are also responsible to ensure that data is accurate and kept up to date.

Data should be stored on the network file servers/cloud rather than the local hard drive to enable any data which is lost, stolen or damaged to be restored with its integrity maintained.

All RiverRock PCs are scheduled to be rebooted every Friday at 22:00.

File Storage and Naming Convention

All documents and files must be given clear and descriptive titles that will help others to understand what is contained within them. All documents should contain a date and version number.

Printing

Staff must ensure adequate care is taken when printing information, utilising the use of RR's secure printing solution where appropriate.

Data Destruction Policy

Information which is no longer required should be promptly disposed of either by deletion or archiving or destruction through secure methods (such as shredding for confidential waste). Unless an audit record of versions is explicitly required, previous versions of documents should be destroyed when the new one is created.

Screen Locking

Computer screens must be locked when unattended to prevent unauthorised access and to protect information.

Memory Sticks and Removable Media

Removable media such as USB memory sticks are restricted to authorised use only.

Where use has been approved by the COO, the user may be added to a device exception list for their requirement.

All removable media devices and any associated equipment and software must only be purchased and installed by the IT Department. Non-RiverRock owned removable media devices must not be used to store any information used to conduct official Company business and must not be used with any Company owned or leased IT equipment.

Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

Staff should avoid storing confidential/sensitive data on portable IT equipment.

All removable media devices that are no longer required, or have become damaged, must be returned to the IT Department for secure disposal.

Mobile Devices

It is prohibited to store any Company data on personal mobile devices. All staff must ensure mobile telephones are always kept secure.

Any unauthorised use or loss must be reported to the IT Service desk immediately to enable the Firm to comply with its obligations towards the Information Commissioner's Office and the regulator(s).

Leaving RR Or Moving into Another Role

All users issued with mobile devices are personally responsible for their return on termination of employment.
Human Resources will maintain records of any mobile devices issued to RiverRock staff. The return of such devices will be a prerequisite for leavers to receive their final payslip.

Passwords and Accounts

All staff are given access rights and privileges to the various systems in accordance with their business area and the type of data and platform they are required to use.

Passwords must always remain protected. If it is suspected that a password has become known to someone else, that password must be changed immediately, and the incident must report to the IT Department. Passwords are user specific only and must never be shared with anyone.

Passwords must be a minimum of 8 characters, a combination of upper and lower case with a minimum of one number. Ideally it should also contain a random character such as #@!$.
Common and easily guessable combinations should be avoided.

Passwords must be changed on a regular basis. RiverRock's policy is every 90 days non enforceable due to dual factor authentication measures in place which reduces the risk of password leaks.

A unique log is available on each account which must not be shared with or leaked to anyone else.

Backups

RiverRock IT will ensure that all application servers and Microsoft365 storage services are backed up on a daily, Monthly cycles. All backups must be kept up to date and must be checked on a regular basis to ensure recovery.

Individual PCs are not backed up; therefore, data should be stored on the cloud network drive allocated to each employee, rather than the local hard drive to enable any data which is lost, stolen or damaged to be restored with its integrity maintained.

Network Shared Drives

It is RiverRock's policy to keep data in a secure manner and to only allow authorised access to files to those who require the data as part of their normal duties. Access to individual data areas will only be granted following a written request from the "owners" of that area. Each user is assigned their individual storage area, known as OneDrive. Only assigned users have access to the files in this area unless a user specifically shares the drive with another staff member. One to one sharing of personal work data is permitted internally.

It is not permitted to store any personal music, video, presentations, or photos on the network shared drives or OneDrive. Any of the mentioned files found will be deleted from the network and may warrant disciplinary action against the involved staff.

Viruses

It is the responsibility of all staff to protect the Company's computer systems from viruses. All files received on disc or removable storage from outside RiverRock must be checked for viruses before being used on RiverRock equipment. IT Department should be consulted first.

Individuals must ensure that an effective anti-virus system is operating on any computer which they use to access RiverRock's Infrastructure.

Any emails containing any links received from any unknown or untrustworthy source must not be opened or forwarded and must reported to IT department in person, by phone call or by sending a screen-capture. Suspicious emails must NOT be forwarded.

If any device is infected or is suspected to be, the IT Department should be informed immediately. The system should be turned off and the workstation should not be used until permission is given from the IT Department.
The intentional introduction, sending or downloading of files or attachments which contain viruses, or which are meant to compromise RiverRock's systems, is a serious breach of this policy and may result in disciplinary action which could result in dismissal and prosecution under the Computer Misuse Act 1990.

Network Accounts

RiverRock's IT Department is responsible for the creation and setup of New User Accounts (network logins) and also for email accounts or anything to do at MS365 Exchange upon the notification from

Human Resources. Department managers and/or system owners are often responsible for requesting the granting of access rights to users wishing to access their respective files and systems.

Clean Desk Policy

The safest approach to protect data/information in hard form is the use of a clean desk policy. RiverRock has a clean desk policy in place to ensure that all restricted and confidential/sensitive information is held securely at all times. Restricted and confidential/sensitive data/information or documents should not be left on desks unattended and should be removed from view when unsupervised.

All manual files and paper records should be secured before leaving the office. Where this is not possible or where offices employ "open" shelving, offices must be locked when left unattended. At the end of each day, it is the responsibility of staff to clear their desk of all documents that contain any sensitive information, or any information relating to clients or customers.

Internet

This policy sets out the guidelines for all RiverRock staff and external users (auditors, consultants etc.) who are provided with access to the Internet whether from an office, home, or mobile broadband connection and from any device.

Provision

The Internet is provided primarily for business use. Reasonable personal use will be permitted if it does not interfere with the individual's delivery of their duties or breach any requirements of this policy and is undertaken in a free time.

Downloading of Information Resources

Individuals may download information including PDFs and Microsoft Office files from the Internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.

Graphical, audio and video files may be downloaded and stored on RR network provided their use is for business only.

Individuals requiring any new software, including any plug-ins, must make a formal request under due approval from line management to the IT Department. Software must not be downloaded and/or installed onto RiverRock IT equipment unless it has been approved by IT and can be validated that it is licensed for current use.

Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any RiverRock work.

Uploading Data/Information to The Internet

Any individual who carries out this function must be sure that the information is suitable and not confidential or personal. To ensure always ask IT or Compliance for assistance.

Prohibited Activities

Individuals are explicitly prohibited from using RR's internet connection to undertake the following activities:

- Accessing gambling sites, spread betting or share dealing
- Conducting private/freelance business
- Looking at pornographic or offensive images/material
- Accessing sites that promote hatred or intolerance based on race, religion, sex, sexuality, or other characteristics that are protected by law
- Accessing militant or extremist resources
- Attempting to gain unauthorised access to private networks (e.g., hacking)
- Any other unlawful or illegal activity.

Anyone indulging in any of the prohibited activities may be subject to disciplinary action.

Internet Filtering and Blocking

RR uses internet filtering to ensure that the Internet is used safely, efficiently, and primarily in connection with RiverRock business. This software monitors internet use and restricts access to various categories of websites. A standard web page explaining that access has been blocked or restricted will be seen by users. Individuals who encounter a commonly used business site which is blocked and have genuine business reasons for accessing that site frequently may contact the IT Department and request the site is moved to an approved list of websites.

Internet Chat Facilities and Social Networking

Subject to their line manager approval-Individuals may access and use approved chat rooms, discussion group's bulletin boards and social networking sites, subject to the following restrictions:

- Access is restricted to a minimum during the working day unless specific permission is granted by your manager.
- Individuals must not give information on a social networking site which is confidential to RiverRock, its suppliers or clients.
- Individuals must refrain from referring on the social networking site to the Company, its staff, its customers, and its suppliers.
- Individuals must not post entries on social networking site which are derogatory, defamatory, discriminatory, or offensive in any way, or which could bring the Company into disrepute.
- Staff should be aware that blogs may create documents which the courts can order to be disclosed for use in litigation. Consequently, staff will be assumed to have written any contentious items from their own opinions and not those of RiverRock unless they can prove definitively that they have not done so.

E-mail

All individuals granted an email account must adhere to the policy contained in **Appendix 1.**

RiverRock has a policy for the use of email whereby the user must ensure that they:

- Comply with Firm policy
- Use email in an acceptable way
- Do not create unnecessary business risk to the company by their misuse of internet.

Staff must ensure recipient email addresses are correct (including distribution lists) so that potentially sensitive or protectively marked information is not accidently released into the public domain.
Staff understand that the RR email account must only be used for work-related purposes and not for personal communications.

Metadata

Definition

While creating, editing, and/or updating a document, certain information may automatically be saved in document file. Such information may be retrieved and used for unauthorised or illicit purposes.
Following metadata may be stored in documents created in all versions of Word, Excel, and PowerPoint etc:

- Name and initials (or those of the person who created the file)
- The name of computer
- Firm or organisation name
- The name and type of the printer
- Document revisions, including deleted text that is no longer visible on the screen
- Document versions
- Information about any template used to create the file
- Hidden text
- Comments

Removing Metadata

Microsoft

I. For sensitive documents disable “allow fast saves” feature.
II. “Inspect Document” and remove flagged items. “Inspect Document” will vary depending on your software version. In office365, it is located under File->Info->Check For issues.
III. Third party software will help identify and clean metadata from your documents if it is necessary to send documents in native format. Verify appropriate software with the IT department.

Converting to PDF

1. Converting files to PDF format with Adobe Acrobat or other PDF creators will usually strip out most metadata.
2. In Acrobat, Select File, then Document Properties to view the summary metadata information within a PDF file. Add further restrictions on how the document can be accessed, used, copied, and printed in the Security Options settings as needed.

Cyber Security

Social engineering and human errors are the biggest cyber security threats. It is of the upmost importance to all possible take security measures to protect your computer information, reduce identity theft and prevent malicious cyber-attacks. With cyber-attacks on a continuous rise, it is crucial to understand and learn ways to prevent these attacks. Knowledge of how cyber-attacks operate and what protective steps can be taken to reduce the chances of that occurrence are key to RiverRock.

Cyber-Attack

A cyber-attack is when someone gains or attempts to gain unauthorised access to a computer maliciously damaging systems or stealing valuable information from that computer.

Cyber-attacks are sent from one computer or network to another with the intent of compromising the target computer or network. Cyber-attacks because security concerns for using the internet safely considering the adverse outcomes of such attacks. Cyber-attacks are dangerous mainly due to their ability to target victims across the globe. This allows for the growth of cyber-attacks to continue generally untamed and difficult to trace. Cyber-attacks cannot be stopped completely since new exploits are discovered every day.

Different Types of Cyber-Attacks

Following are some of the most common types of cyber-attacks:

Malware

Malware is known as any computer code created for causing malice. Malware is capable of infecting computer systems, slowing or shutting them down and stealing valuable information. Malware continues to grow limitlessly along with cyber-attacks, and it is a popular tool in cyber-attacks. It is contagious and able to quickly spread across the web, as it is a small file with capabilities of infecting whole file systems. Malware can cause more harm the longer it exists in your system. For this reason, it is important to protect against, detect and eliminate malware from your computers.

Malware has three common forms:

- Spyware
- Viruses
- Worms

Ransomware

Ransomware is a type of malicious software which blocks access to a computer system or encrypts digital files so no one can access it/them without paying a fee. The malicious software displays a message about how the user can supposedly regain access to his/her system/files by paying a ransom. There is no guarantee paying the ransom will allow the user to regain access to those files.

Password Attacks

As computer users, passwords serve essentially as keys to all our private information. When the password is lost, it must be reset quickly to prevent the risk of theft. It is important to understand how hackers can

'steal' passwords from unsuspecting victims. Some methods of password attacks include password guessing, password resetting and password capturing.

DDos Attacks (Distributed Denial of Service Attacks)

A DDos attack is used to hack websites and companies' data servers. These attacks work based around the principle of overloading a computer system or server. Overloading the system leads to slowing down or even shutting down servers entirely. If a DDos attack is severe enough it can be used as a distraction from other security vulnerabilities which can lead to stolen information.

Pop-Ups

Pop-ups are a major component and a common feature of web browsing. Many reputable organizations use pop-ups for multiple legitimate purposes. However, cyber-attacks have occurred where the hackers generate a fake pop-up which can appear even if a reputable companies' website is being browsed.

Public Unsecured Wi-Fi Network Attacks

Public Wi-Fi networks are generally seen as convenient to most users. Public Wi-Fi is common in hotels, restaurants, shopping centres, airports, and many other places. These public networks are convenient however they are not password secured. Public networks are at much greater risk for cyber-attacks than networks which are private, and password protected. Cyber-attacks can target these networks and monitor or steal valuable information sent over these networks.

Phishing Scams

Many people using e-mail have probably received an e-mail of some ridiculous lottery winning from other countries or various other scams asking for personal information. Phishing are fake emails made to look legitimate asking information for malicious purposes.

Man-in-Middle Attacks

Whenever information is shared over the internet, it is transported through multiple networks before reaching its destination. A Man-in-Middle attack intercepts the data as it is going through these various networks. These attacks can be very difficult to detect as it is still possible for the data to reach its destination.

Eavesdropping

It is an unauthorised real-time interception of a private communication, such as a phone call, email or video conference. Unlike the Man-in-Middle attack, eavesdropping simply monitors the information being sent from the client to the server. Information is not sent to another computer in the case of eavesdropping. Many users may not be able to realise whether a network connection is being eavesdropped however, there are precautions to limit the changes of such an occurrence.

Session Hijacking

Session Hijacking is a type of cyber-attack in which a valid session between a client and server is temporarily used, therefore giving he name "Hijacked" for malicious purposes. This works by the way of using a valid client's cookie which is authenticated by the server to connect to the it. Once a valid connection is established the client's information that is transferred to the server can be accessed. Ensure the reputation of the company receiving the information, as well as checking the server's security for

proper certification. Giving information to servers without checking these simple prerequisites can lead to an almost undetectable information loss.

Methods to Prevent Cyber-Attacks

Some of the most common and effective methods to prevent cyber-attacks include:

Choosing Strong Different Passwords

The importance of selecting a strong password cannot be emphasised enough since it is a key to the private data. It is essential to use different passwords for different accounts. When someone uses the same password for all accounts, if that password was to be stolen, thieves would have access to multiple different accounts as opposed to someone who uses a different password for each account.

Keeping Your Information Confidential

Sometimes preventing cyber-attacks is as simple as using common sense. One needs to be wary of giving out information to random/untrustworthy websites. Giving up valuable information to such organizations can easily lead to identity theft and fraud. E-mail is a popular way for hackers to spread malware and Trojans to a computer.

Installing And Periodically Running Antivirus Software

The first measure you need to take in protecting your computer is to install anti-virus software on the system, RiverRock has these installed on all computers. Antivirus software detects, prevents, quarantines, and removes malicious computer programs from the system.

Avoiding Public Wi-Fi

Public Wi-Fi is vulnerable and as dangerous as it is convenient. Since public Wi-Fi is unprotected, it should be avoided unless necessary. When used, no information of any kind should be sent over such networks. Avoid transactions or registering for anything that requires any input of personal information.

Safe Browsing

Be wary of using websites that have no security measures in place for personal information. Most websites will show links to the security certificate if information is encrypted. One can simply check for such certificates to assist in deciding whether the organisation can be trusted with information.

Keeping Software Up to Date

Software updates are essential to proper security since no application is 100% impenetrable. Most software includes automatic updaters which allow updates to complete with a few clicks of the mouse.

Firewalls

Firewalls are applications that check for any information that is communicated from your computer with anyone else. Firewalls are guards against any unwanted communications from any source. Firewalls are an essential second layer of protection against any types of cyber-attacks.

Avoiding Free Software Downloads (Freeware)

You need to be more responsible when it comes to downloads. Not all freeware is malicious however, it can carry viruses and other forms of malware along with it. Use antivirus software to scan any software downloads (not just freeware) in order to check whether the software should be installed.

Data Encryption

Files can be encrypted to ensure that if these files were to ever fall into someone else's hands, information cannot be accessed. It prevents the hacker from modifying, changing or getting access to the personal files/documents.

E-mail Security

It defends against spams, blocks phishing, viruses, malware, protects privacy and data loss with automatic encryption. E-mail is a popular way for hackers to spread malware and Trojans to a computer. To ensure your computer does not get affected:

- Do not open unknown e-mail attachments or respond to unknown e-mails
- Do not respond to online requests for personal identifiable information
- Let anti-virus scan email attachments prior opening
- Never open emails from spam box
- Never forward such emails to the IT department; inform them separately
- Never click on a suspicious link send in an unknown email

How to Deal with a Cyber-Attack

- Find out if your computer has any suspicious activity
- Report to the IT immediately for professional assistance and immediate actions to minimise the effect of any level of cyber attack
- Fix the problem and try to restore the computer to service
- Unplug the internet cable and shutdown the infected machine immediately
- Take the computer to a certified computer technician

IT Infrastructure, Data & Information Security Risk Assessment

RiverRock shall develop, implement, and promote an effective and responsive security risk assessment mechanism that ensures that all IT infrastructure, data, and information shall proactively be assessed to identify, assess, mitigate, and monitor potential risks.
Such security risk assessment mechanism shall, at minimum, ensure that IT risks are effectively managed at all levels.

Three most important factors in security risk assessment are:

IT Asset - the importance of the assets at risk,
Threat - how critical the threat is, and
Vulnerability - how vulnerable the system is to that threat.

Risk = Asset **x** Threat **x** Vulnerability

Using these factors, IT risks shall be assessed, prioritized, mitigation plan designed and implemented, and continuously monitored.

Security risk assessment process shall comprise of following steps:

Asset Identification and cataloguing

Identifying and recording all IT assets across the Firm that could be exposed to risks that if materialize might affect organizational goals

Threat & Vulnerability Identification

Identifying potential threats (such as ransomware, customer data leakage etc.) and vulnerabilities (such as outdated security patches, human negligence, unauthorised access) that might affect business operations and objectives

Risk Assessment

Conducting inherent & residual risk assessment to assess the likelihood and severity of identified risks to measure impact on given processes and business operations. Risks shall be categorised on 5x5 risk matrix of likelihood and severity. (Annex. A)

Risk Prioritization

Prioritizing risks based on potential likelihood and impact.

Risk Treatment

Identifying or creating and implementing risk treatment strategy to mitigate or transfer the potential impact

Risk Monitoring

Monitoring and evaluating the risk levels and the effectiveness of risk treatment strategies already implemented

Risk Reporting

Periodically reporting risks and control to different stakeholders

Unacceptable Behaviour

The following behaviour is considered unacceptable:

- use of Company communications systems to set up personal businesses or send chain letters
- forwarding of Company confidential messages to external locations, including the user's personal email address, without prior senior management approval
- distributing, disseminating, or storing images, text or materials that might be considered indecent, pornographic, obscene, or illegal
- distributing, disseminating, or storing images, text or materials that might be considered discriminatory, offensive, or abusive, in that the context is a personal attack, including without limitation, a sexist or racist attack, or which otherwise might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the Company's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business-related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the corporate network

Remote Working

Any portable device, such as a laptop or smart mobile/tablets must be kept in a secure location when not in use. When using equipment on the move, or outside of office hours, reasonable care should be taken to secure it. Equipment should only be left unattended when necessary and after additional steps have been taken such as locking the laptop in a secure, non-visible place. Laptops should not be taken into busy social areas or where it may be difficult for the user to keep always hold of the equipment, and care should be taken to avoid being overlooked whilst using RiverRock equipment or accessing RiverRock systems in any public area.

Any portable computing equipment must not be left unattended during the normal working day unless it is on RiverRock premises where there is good physical security at entrances to the building. Outside of normal office hours and when the building is closed, all portable computing equipment left on office premises should be kept in a locked cupboard or similar storage.

Portable computer equipment containing sensitive, or client data shall only be removed from the RiverRock's premises where necessary. Where it is necessary for sensitive or client data to be processed and stored away from RiverRock's premises, individuals should inform and record this step with their manager.

Where manual files are processed outside of RiverRock's property they should be kept with the individual completing this work wherever possible. When left unattended they should be in a locked container and out of view. Any computer equipment or manual files that are travelling with a member of staff should be locked in the boot of the car or always kept with the individual when travelling by public transport. Under no circumstances should any computer equipment or manual files be left unattended on public transport or left in a vehicle overnight.

Any member of staff who has been authorised to work from home (WFH) will be allowed, by default, to connect their personal computer to RiverRock's network. This is as secure as connecting directly to the network in a RiverRock office using the local area network (LAN).

Incident Reporting

Any breaches of security (defined as non-compliance with this policy), however minor, must, at the earliest, be reported to the line manager and the IT department, providing all necessary information such as incident nature, location, time of incident, potential severity of the incident etc.

Loss of any piece of IT equipment (computer, laptop, mobile phone, USB storage device, etc.), is classed as a security incident and should be reported as outlined above and copied to the COO.

Management of User Accounts: Leavers

Managers are responsible for ensuring that all IT equipment is returned to RiverRock's IT Department on the day of departure and to ensure that their IT account is disabled immediately after their departure. Prior to the account being disabled, managers are to ensure that the user's work-related information, e-mails and data is transferred, if required, to the respective working directory for future access on the system or is deleted. This will ensure that the appropriate security is maintained on leavers' information and data.

All RiverRock owned IT equipment must be handed back to the IT Department.

User's Responsibilities

- Everyone must ensure that no unauthorised person has access to any data held by RiverRock. Each person must ensure that any physical security measures are properly used.
- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to RiverRock. This includes the spreading of viruses or other similar computer programmes.
- Individuals will be given access passwords to certain computer systems. These must not be disclosed to other members of staff. They should not be written down, and must not be stored on the network, and they should be changed regularly.
- Staff shall not load or download software packages onto their PCs. This must only be carried out by IT Department. On no account must games software be loaded on staff PCs.
- Staff are not permitted to store personal documents or files on the RiverRock network drives. Any staff found to be storing large numbers of personal files, especially large files such as photographs or videos will be asked to remove them.
- Any files received on any media, brought, or sent into RiverRock or files received by electronic mail must be virus checked before being loaded onto a RiverRock PC. This includes any media which have been used on machines at home or otherwise not on RiverRock's premises. For assistance with this, please contact the IT Department.

- Individuals must not leave their computer unattended when it is logged on. Whenever you move away from your workstation ensure you log off or lock your workstation (locking can be achieved by simultaneously pressing the Control, Alt and Delete keys once and selecting “Lock Computer”).

Manager’s Responsibilities

- All managers must give their full backing to all the guidelines and procedures as set out and agreed in this document.
- Certain managers, where they have responsibility for individual systems, must maintain records of users of that system and control their access to it by allowing access privileges. They must:
    - check the user has authorisation to use the service (including that the user has a valid CRB check where this is relevant).
    - check the level of access is the minimum level appropriate for the business purpose and is consistent with this security policy.
- The granting of user access to RiverRock network can only be carried out by the IT Department. For some line of business systems, the manager is responsible for allowing access.
- Managers must make the IT Department aware of all new staff (requiring access to any IT equipment) so that log-in rights and access privileges can be set as appropriate. This is part of RiverRock’s New Starters process.
- Where staff do not have sufficient knowledge to be able to use systems efficiently and securely their managers must ensure that appropriate training is arranged before allowing them access to RiverRock’s computer systems. Advice to managers in making this assessment can be obtained from the IT Department.
- Managers must also take responsibility to ensure:
    - all staff receive a briefing on this policy as part of their induction programme within two weeks of joining RiverRock.
    - all staff are aware of the strict confidentiality of the information to which they will have access.
    - staff always use the information in an appropriate manner.
- It is up to all managers of staff in RiverRock to ensure that individuals adhere to these procedures. The IT Department and Compliance Team will be responsible for monitoring systems for signs of:
    - Illegal or unauthorised software having been loaded.
    - Password misuse.
    - Unauthorised access
- Spot checks will also be made to ensure that where data is not held and backed up centrally, adequate backups are being made.

Appendices

Appendix 1: Use of Email and Calendar

Outlook is a useful tool that enables individuals to organise themselves and communicate with others. This policy sets out the expectations for all RR computer equipment users who are provided with access to Outlook. Outlook is provided as a business tool and should not be used for non-work-related matters. Individuals with a need to send personal mail during working hours must do so using personal webmail accounts (such as Hotmail or Google mail).

Mailbox Size and Housekeeping

The standard individual mailbox size provided is 50GB. In addition to individual mailboxes, shared mailboxes can be provided where there is a specific business need. Please contact the IT Department for assistance. Once the mailbox limit is reached, users of that mailbox will not be able to send or receive any further mail and therefore housekeeping must be planned well in advance of reaching the space limit. User level Email archive is good practice and can be enabled if required at our Exchange365. All emails are archived at our Mimecast server.

Distribution Lists

Mail distribution lists are provided to enable business communications to be made to groups of individuals, and each list must have a designated owner. Lists should only be used for related business purposes, and any queries related to their use or composition should be directed to the list owner in the first instance. Users may not use the "All RiverRock" distribution list without permission from the CEO or the CFO/COO.

Mailbox Management

Individuals are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate.
Individuals should only archive and retain messages that need to be kept and these should be selected in line with business needs and any corporate retention schedules that may exist. All other e-mail that does not constitute a necessary record of business should be deleted once it is no longer required.

When an email is received with an attachment which needs to be retained, individuals should save the attachment to the departmental cloud network drive, and not leave the attachment within the email where possible.

Sending Email

All e-mails must have the subject line completed and should be checked for accuracy of spelling, punctuation, and grammar. Bold text should only be used sparingly, and for emphasis, and underlining should only be used for links. The use of upper-case text should be avoided as this may be interpreted by recipients as shouting.

To avoid information overload, individuals should consider carefully who needs to be included in any e-mail and whether face-to-face or telephone/MS Teams contact could be an alternative method. When sending confidential or sensitive e-mail, individuals should be mindful of any delegate permissions that recipients may have set up.

Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.

Individuals must not use other people's mail accounts (unless they have authority to do so) nor attempt to impersonate someone else or appear anonymous when sending e-mail.

All external emails should be finished with an email signature that includes your name, title, and contact details.

Agreements By Email

Individuals should take care not to enter into any agreements via e-mail that could constitute a contract, and if in doubt must seek the advice of RR Legal and Compliance.

Misuse Of Email

Individuals must not send or forward any abusive, threatening, defamatory or obscene messages. Likewise, individuals should avoid sending messages in the heat of the moment, taking time to reflect on drafts and how they may be interpreted before sending them.

RR has spam filtering software in place to help reduce the volume of unsolicited e-mail. However, such software is not infallible, and individuals should therefore take care with any suspected malicious or nuisance e-mails (e.g., chain e-mail, hoax and spam e-mails) they receive, ideally deleting them. Individuals must also never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

Mail And Absence

The "out of office" notice may be used whenever an individual is away from their normal office base and is checking messages less frequently than normal; in this case messages should clearly indicate a date of return to the office and contact details for those who can deal with issues whilst the individual is away. Individuals with a Blackberry should note that they can turn on or switch off out of office using their Blackberry.
In the event of an unforeseen absence where there is a need for the "out of office" function to be turned on, the manager should provide the IT Department with the required text.

To protect individual privacy, access to other individuals' mailboxes is not normally provided. Where there is a business need for emergency temporary access, this can be provided with the individual's explicit written consent. In the absence of consent, the manager should contact the IT Department for advice. The IT Department will not be able to arrange access without seeking permission from senior management.

Calendar

To help with setting up meetings and locating colleagues, calendars should be set to be viewable by authorised users. Consequently, it is important that individuals use the "private" option for all confidential appointments. If you are unsure how to do this, please contact the IT Department.

Individuals are required to keep their calendars up to date and must indicate their whereabouts when away from their normal office base.

Appendix 2: References

Legal references

- Computer Misuse Act 1990
- Data Protection Act 1998
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

This list is not exhaustive and may be subject to additions or deletions to be approved by RiverRock from time to time.
In case of any queries about this policy, in the first instance, speak to IT Head or Compliance Officer.

Policy Compliance

Breach of this policy may result in disciplinary proceedings, up to and including dismissal with immediate effect or termination of contract with immediate effect. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
If you do not understand the implications of this policy or how it may apply to you, seek advice from the Compliance Officer or the IT Head.

Annexure A:

IT Infrastructure, Data, & Information Security Risk Assessment Matrix

RATING	DEFINITION
NEGLIGIBLE	A risk event that, if it occurs, will have **little or no impact** on achieving outcome objectives.
LOW	A risk event that, if it occurs, will have a **minor impact** on achieving desired results, to the extent that one or more stated outcome objectives will fall below goals although well above minimum acceptable risks.
MODERATE	A risk event that, if it occurs, will have a **moderate impact** on achieving the desired results, to the extent that one or more stated outcome objectives will fall well below goals but above minimum acceptable levels.
HIGH	A risk event that, if it occurs, will have a **significant impact** on achieving the desired results, to the extent that one or more stated outcome objectives will fall below acceptable levels.
EXTREME	A risk event that, if it occurs, will have an **extreme impact** on achieving the desired results, to the extent that one or more of critical outcome objectives will not be achieved.