CYBER AND INFORMATION SECURITY POLICY

Technical Rescue International

V1.2019

TRI CYBER SECURITY GUIDELINES

State and non-state actor sponsored cyber-attacks are a risk to all organisations and need to be taken seriously. Please read the following document extremely carefully.

SECURITY PLANNER

1. Go to the website www.securityplanner.org and begin the questionnaire.
2. Select all options that apply to you – both at home and at work. Note that this should be the majority of the options available.
3. Follow the recommendations given.

TRI SECURITY

- As the Security Planner will have told you, it is of vital importance that you enable Two Factor Authentication wherever possible – certainly on all email and social media platforms.
  - This can either be via SMS or via an Authenticator – e.g. Google Authenticator. The latter is recommended if you travel or have multiple SIM cards.
- Do not remain logged in to websites.
- Passwords specifications:
  - 16 character minimum
  - Must include all of the following: Lower Case letters; Upper Case letters; Numbers; Symbols.
  - You must not use the same password for different tools.
- Note that if your iCloud account is compromised, the attacker may use it to gain access to many of your other devices and platforms.
- NEVER INSERT A USB DRIVE OR OTHER EQUIPMENT WITHOUT KNOWING WHERE IT HAS BEEN. Attackers have hacked a number of companies by leaving USB drives loaded with malicious software in the office, which gained access to company networks when the USBs were inserted into computers by well-meaning employees. Always make sure of your personal drives.

PHISHING ATTACKS

'Phishing' is a method by which someone may try to obtain sensitive information from you. A phishing attack comes disguised as a trusted source – like Microsoft Outlook – and will ask you to follow a link, enter your password or other personal information.

A number of UK based organisations have received several phishing attacks in the past, and it is highly likely that more will come. You must be extremely vigilant, and report every suspicious contact to your line manager.

RECOGNISING A PHISHING ATTACK

It is important to note that phishing attacks can be highly sophisticated and need no longer look like a typo-ridden email from an uncle in Nigeria claiming that you have inherited half a million dollars. Every email should be treated as a potential attack, and the following steps taken to identify it:

- DO NOT CLICK ON ANY LINK OR ATTACHMENT UNTIL YOU ARE CERTAIN THAT THE MESSAGE COMES FROM A VERIFIED SOURCE.
- Hover your mouse cursor over the address from which the message was sent. The full address will appear – make sure it is a trusted source.
    - Note that there are many ways in which a trusted source may be faked:
        - Microsoft might be written Microseft, or Micr0s0ft – and in certain fonts, those can look almost identical to the real spelling. GMAIL might be written GMAlL. Etc. etc.
- Hover your mouse cursor over the link. The address will appear – follow the above steps again.
-

If one of your colleagues or friends is compromised, you may receive phishing attacks directly from their address. It is important to always check the actual link in an email, even when it comes from a trusted source.

Attackers may identify the equipment we use in the office. This would enable them to disguise their attacks as a message from the office printer or from another service that we use. No mail is safe until you have checked it properly.

WORKING REMOTELY

DO NOT USE PUBLIC WIFI (CAFÉ, AIRPORT, HOTEL) WITHOUT A VPN. A VPN (Virtual Private Network) masks your IP address and makes it impossible for someone on the same network as you to access your computer. A free VPN for Google Chrome is Betternet. A download link can be found here:

https://chrome.google.com/webstore/detail/betternet-unlimited-free gjknjjomckknofjidppipffbpoekiipm

It is recommended, however, that you purchase a full service like NordVPN or ExpressVPN. These will better protect your computers as well as your phones and other devices.

PHYSICAL SECURITY

- Make sure never to leave your devices unattended, especially when unlocked. This applies just as well to conferences and workshops as cafes.
- Of course, never allow any of your devices to be accessed without a password.
- Never write your username or passwords on paper to be kept somewhere.
- Encrypt your hard drives. This is easily done on Macs using FileVault.
    - Select System Preferences -> Security & Privacy
    - Select FileVault.
    - Click the padlock symbol in the bottom left corner and enter your admin details.
    - Click Turn On FileVault.
    - For more details, see here:
        - https://support.apple.com/en-us/HT204837

GENERAL ADVICE FOR SAFER WEB BROWSING

- Be conservative with online downloads.
- Beware antivirus scams.

- Interact only with well-known, reputable websites.
- Confirm each site is the genuine site and not a fraudulent site.
- Determine if the site utilizes SSL (Secure Sockets Layer), a security technology for establishing
- Encrypted links between Web servers and browsers.
- Don't click links in emails—go to sites directly.
- Use social media best practices.

TECHNICAL RESCUE INTERNATIONAL INFORMATION SECURITY POLICY

Policy

It is the policy of Technical Rescue International (TRI) that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for 10 (ten) years after initial creation, or, pertaining to policies and procedures, after changes are made.

Scope

Information security is designed to protect the confidentiality, integrity and availability of information.The framework for managing information security in this policy applies to all companies within the TRI organisational structure and their employees. This policy applies to all corporate information and other classes of protected data in any form as defined below.

Risk Management

A thorough analysis of all TRI information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats (internal or external, natural or manmade, electronic and non-electronic) that affect the ability to manage the information resource and will also document the existing vulnerabilities within each company. The analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection. From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

INFORMATION SECURITY DEFINITIONS

- Availability: Data or information is accessible and usable upon demand by an authorised person.
- Confidentiality: Data or information that is not made available or disclosed to unauthorised persons or processes.

- Integrity: Data or information that has not been altered or destroyed in an unauthorised manner.
- Involved Persons: All employees of TRI and associated partner companies.
- Involved Systems: All computer equipment and network systems that are operated within the TRI environment. This includes all platforms (operating systems), all computer systems (desktops, laptops, tablets, smartphones etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
- Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

INFORMATION SECURITY RESPONSIBILITIES

Information Security Officer. The Information Security Officer (ISO) at TRI is responsible for the development and implementation of security policies, procedures and controls. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered to.
2. Providing basic security support for all systems and users.
3. Advising owners in the identification and classification of computer resources.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing on-going employee security education.
7. Performing security audits.
8. Reporting regularly to the TRI Director regarding information security.

Information Owner. The owner of a collection of information is the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of a Programme or Project within TRI. In this context, ownership does not signify proprietary interest and ownership may be shared. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from the Compliance Department (normally 10 years).
3. Ensuring appropriate procedures are in effect to protect the confidentiality, integrity and availability of the information used or created within the unit.
4. Authorising access to information. Assigning access will be carried out by the IT department.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of TRI information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilising programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organisational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

IT Manager. The IT Manager is responsible for the processing and storage of the information and is responsible for the administration of controls as specified by the ISO. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorised by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
7. Promoting employee education and awareness by utilising programs approved by the ISO, where appropriate.
8. Reporting promptly to the ISO the loss or misuse of TRI company information.
9. Identifying and responding to IT security incidents and initiating appropriate actions when problems are identified.

Management of Information Users. The management of Information Users will be carried out by line managers who supervise users as defined below.

1. Reviewing and approving all requests for their employees access authorisations.
2. Initiating security change requests to keep employees' security record current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with termination procedures.
4. Revoking system access to terminated employees.
5. Identifying the IT training needs of the employee.
6. Reporting promptly to the IT Manager the loss or misuse of TRI company information.

Information User. The Information User is any person who has been authorised to read, enter or update information. The Information User is expected to:

1. Access information only in support of their authorised job responsibilities.
2. Comply with Information Security Policies and Standards.
3. Keep personal authentication methods (e.g. passwords, PINs, etc.) confidential.
4. Report promptly to their line manager the loss or

INFORMATION CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity of all TRI information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in any format (e.g., source document, electronic record, report) must have

the same classification. The following levels are to be used when classifying information:

Confidential Information

1. Confidential Information is by definition important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Examples of Confidential Information include: personnel information, key financial information, proprietary information belonging to donors or sponsors, system access passwords.
2. There is to be no unauthorised disclosure of this information to people without a business need as it may cause significant problems for TRI, its donors, beneficaries, or its business partners. Decisions about the provision of access to this information must always be cleared through the Information Owner.

Internal Information

1. Internal Information is intended for unrestricted use within TRI, and in some cases within affiliated organisations such as donors, beneficaries and business partners. Examples of Internal Information may include: personnel directories, internal policies and procedures and programme / project related documents. Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Information.
2. There is to be no unauthorised disclosure of this information unless authorised by the Information Owner.

Public Information

1. Public Information is information that has been specifically approved for public release by a designated authority within TRI. Examples of Public Information may include programme related reporting, marketing brochures and material posted to the TRI website.
2. This information may be disclosed outside of TRI.

COMPUTER AND INFORMATION CONTROL

All Involved Systems and information are assets of TRI are expected to be protected from misuse, unauthorised manipulation, and destruction. These protection measures may be physical and/or software based.

Ownership of Software: All computer software developed by TRIemployees or contract personnel on behalf of TRI or licensed for TRI use is the property of TRI and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Installed Software: All software packages that are loaded on computers and networks within TRI must comply with applicable licensing agreements and restrictions and must comply with TRI acquisition of software policies.

Virus Protection: Virus checking systems have been approved by the Information Security Officer and must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorised to turn off or disable virus checking systems.

Access Controls: Physical and electronic access to Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by employees, a variety of security measures will be instituted as recommended by the Information Security Officer. Mechanisms to control access to Confidential and Internal information include (but are not limited to) the following methods:

Authorisation: Access will be granted on a "need to know" basis and must be authorised by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

1. Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.
2. Role-based access: An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organisation's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
3. User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their UserID.

1. At least one of the following authentication methods must be implemented:
   a. strictly controlled passwords (See Password Policy)
   b. biometric identification, and/or
   c. PIN access (smartphones).
2. The user must secure his/her authentication control (e.g. password, pin) such that it is known only to that user and a designated security manager.
3. An automatic timeout re-authentication method (Password enabled screen saver) must be implemented on all systems.
4. The user must either lock their account, log off or secure the system when leaving it.

Data Integrity: TRI must be able to provide corroboration that Confidential, and Internal Information has not been altered or destroyed in an unauthorised manner. Listed below are some methods that support data integrity, under the control of the ISO:

1. Transaction audit
2. Disk redundancy (RAID)
3. ECC (Error Correcting Memory)
4. Checksums (file integrity)
5. Encryption of data in storage
6. Digital signatures

Transmission Security: Technical security mechanisms must be put in place to guard against

unauthorised access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

1. Integrity controls and;
2. Encryption, where deemed appropriate.

Remote Access: Access into the TRI network from outside will be granted using approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the TRI network.

Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorised individuals. The following physical controls must be in place:

1. Server based systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
2. File servers containing Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorised individuals.
3. Workstations or personal computers (including laptops, tablets and smartphones) must be secured against use by unauthorised individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:
    a. Position workstations to minimise unauthorised viewing of protected information.
    b. Grant workstation access only to those who need it in order to perform their job function.
    c. Establish workstation location criteria to eliminate or minimise the possibility of unauthorised access to protected health information.
    d. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to Confidential Information.
    e. Use automatic screen savers with passwords to protect unattended machines.
4. Access controls have been implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorised access is allowed. Local policies and procedures must be developed to address the following access control requirements:
    a. Contingency Operations – Access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
    b. Facility Security Plan – Safeguarding the facility and the equipment therein from unauthorised physical access, tampering, and theft.
    c. Access Control and Validation – To control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programmes for testing and revision.
    d. Maintenance records – To document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

Emergency Access:

1. TRI has established a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

2. Procedures are documented to address:
   a. Authorisation,
   b. Implementation, and
   c. Revocation.

3. Equipment and Media Controls: The disposal of information must ensure the continued protection of Confidential and Internal Information. TRI has developed and implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain Confidential Information into and out of a facility and the movement of these items within the facility. The following have been addressed:
   a. Information Disposal (Shredding):
      i. Hard copy (paper)
      ii. Magnetic media (hard drives, usb sticks etc) and
      iii. CD ROM Disks
   b. Accountability: TRI maintains an inventory of hardware and electronic media.
   c. Data-Backup and Storage: When needed, create a retrievable, exact copy of electronic Confidential Information before movement of equipment.

4. Other Media Controls:
   a. Confidential Information stored on external media (cd-roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorised access. The External Storage Media must be encrypted. Such media must be appropriately labeled so as to identify it as Confidential Information. Further, external media containing Confidential Information must never be left unattended in unsecured areas.
   b. Confidential Information must never be stored on mobile computing devices (laptops, smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:
      i. Power-on passwords
      ii. Auto logoff or screen saver with password
      iii. Encryption of stored data or other acceptable safeguards approved by Information Security Officer.
      iv. Further, mobile computing devices must never be left unattended in unsecured areas.
   c. If Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of TRI Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with TRI.

5. Data Transfer/Printing:
   a. Electronic Mass Data Transfers: Downloading and uploading Confidential and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research purposes that include Confidential Information must be approved through Line Management with direction from the

ISO. All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place when transferring Confidential Information to external entities.

b. Other Electronic Data Transfers and Printing: Confidential and Internal Information must be stored in a manner inaccessible to unauthorised individuals. Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. Confidential Information that is downloaded for educational purposes where possible should be de-identified before use.

6. Oral Communications: TRI staff should be aware of their surroundings when discussing Confidential and Internal Information. This includes the use of cellular telephones in public areas. TRI staff should not discuss Confidential or Internal Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

7. Audit Controls: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Confidential Information must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for ten (10) years.

8. Evaluation: TRI requires that periodic (3 monthly) technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic Confidential Information to ensure its continued protection.

9. Contingency Plan: Controls must ensure that TRI can recover from any damage to computer equipment or files within a reasonable period of time. TRI will develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Confidential or Internal Information. This will include developing policies and procedures to address the following:

a.Data Backup Plan:

i. A data backup plan will be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.

ii. Backup data will be stored in an off-site location and protected from physical damage.

iii. Backup data will be afforded the same level of protection as the original data.

b. Disaster Recovery Plan: A disaster recovery plan must be developed and documented containing a process to restore any loss of data in the event of fire, vandalism, natural disaster or system failure.

c. Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

d. Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

e. Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

COMPLIANCE

The Information Security Policy applies to all users of TRI information including: Directors, members of the Senior Management Team, employees, contractors, consultants, temporaries, volunteers, interns and outside affiliates. Failure to comply with Information Security Policies and Standards by the aforementioned parties may result in disciplinary action up to and including dismissal in accordance with applicable TRI procedures, or, in the case of outside affiliates, termination of the affiliation.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorised disclosure of Confidential Information as specified in Confidentiality Statement.
- Unauthorised disclosure of a sign-on code (user id) or password.
- Attempting to obtain a sign-on code or password that belongs to another person.
- Using or attempting to use another person's sign-on code or password.
- Unauthorised use of an authorised password to invade patient privacy by examining records or information for which there has been no request for review.
- Installing or using unlicensed software on TRI computers.
- The intentional unauthorised destruction of TRI information.
- Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.