



Cyber Security Requirements for Contractors

Cyber security is something that RUSI takes seriously, both as a topic for research, and internally to protect RUSI information and computers. Whilst the Institute does everything that it can to ensure good cyber security through technology and training, it is vital that everyone with access to RUSI systems, and everyone that works with RUSI, also takes responsibility. Effective cyber security hinges on effective user behaviours.

This document is specifically about cyber security and ensuring that neither the individual nor RUSI is compromised. You are expected to follow the guidance in this document at all times when under contract with RUSI, when using RUSI systems, or when handling RUSI information, such as emails, on your devices.

If you are unable to follow this guidance, you must make RUSI aware immediately. By signing your contract with RUSI, you are confirming that you are able to follow this guidance and that you will do so for the duration of the contract and even after the contract ends if you continue to work with RUSI.

In exceptional cases, you may be issued with a RUSI email address in the course of your work. If that is the case, additional guidance will be provided, and you must attend a cyber-security training session arranged by RUSI.

Email

Email is a favoured means of attack for the whole range of cyber threat actors. Although there are technical defences for malicious emails, they can only ever be partially successful: effective security requires the end user to be vigilant and to treat any suspicious emails with care. Whatever platform you choose to use for email services, you must ensure your email account is protected by multi factor authentication (see below).

Passwords

Passwords are an important component of cyber security. It is important, when signing up for online services, that you have a unique password for each of them. Complex passwords are also better, but a unique password is a must and long passwords are always a good idea.

By far the easiest way to manage your passwords is to use a piece of software called a password manager. These are an encrypted store of all your usernames and passwords, and even better, they will generate unique, strong passwords for you to use with each service.

You **must** ensure you take care when choosing passwords:

- Passwords **must** be unique. You must not reuse passwords on multiple systems or websites.

- Do **not** choose passwords based on information that is easily guessable, or discoverable. Do not include your name, place of work, date of birth etc. in passwords.
- Do **not** use dictionary words, football teams, place names and other commonly used passwords.
- Do **not** use common substitutions e.g. replace the letter 'o' with a zero. Meeting these requirements across a range of websites is challenging, hence the recommendation that you use a password manager. However, you can also write down passwords, provided they are stored securely. If you choose to do this, you **must** ensure you never leave the notebook containing your passwords accessible and unattended. It **must** be stored in a locked cupboard or drawer that only you can access.
- **On no account must** your password be disclosed to anyone else, not even to a trusted colleague.

Multi Factor Authentication

Multi factor authentication is a means of providing additional protection when logging into online services. Typically, you just have a username and password when authenticating to an online service, however, if you have multi factor authentication enabled, you need an additional step to successfully authenticate to an online service. This can be a hard device you plug into your computer, an app on a smartphone that generates a six-digit code, a notification you have to approve to continue with the login, or a text message.

Most large online services, including all the main email providers, social media websites, and cloud storage companies, now support two-factor authentication in one, or more, of these forms. For any RUSI business, two-factor authentication must be enabled, and where possible a hardware or software solution used, rather than a text message.

Device Security Requirements

The following security requirements **must** be met:

- The device must be protected by a PIN, passcode, or biometrics
- The device must be encrypted
- Laptops must have a software firewall enabled
- Laptops must run some form of antivirus or antimalware software
- The device must automatically lock if unattended or unused for a short period, and require a password to unlock
- The device must support remote locking and wiping if lost.
- All devices must be kept up-to-date. Updates, and security fixes to the device operating system must be applied when they are released. Devices that no longer receive security updates, or otherwise run out-dated operating systems, are not permitted.
- RUSI reserves the right to check device compliance where necessary.

Cloud Services/Sharing Files

RUSI's required method for hosting and sharing files is SharePoint (part of the O365 application suite). In exceptional cases we may use Dropbox but only if the Dropbox is set up and administered by RUSI.

Reporting Incidents

RUSI contractors should report any suspicious incidents, such as phishing emails, to their RUSI supervisor and at the email compliance@rusi.org.