Remote Working Policy

POL-088

1. Policy Purpose and Scope

Cyber Criminals are attempting to gain entry to GRAHAM network on a daily basis. These attacks can be launched from anywhere in the world. In order to ensure the confidentiality, security and integrity of the GRAHAM information systems, access controls are vital.

As part of our security measures to protect GRAHAM business, network access from all locations (except UK & Ireland) is permanently blocked.

This policy outlines the acceptable user behaviour when accessing GRAHAM information systems remotely and defines the process for requesting network access from outside UK and Ireland. The policy is part of the overall Information Security Policy and operates in conjunction with the IT Acceptable Use Policy.

This policy applies to employees, contractors, consultants, fixed term employees, and other workers at GRAHAM, including all personnel affiliated with third parties given access to GRAHAM equipment or systems.

This policy applies to all equipment that is owned or leased by GRAHAM. The definition of equipment includes, but is not limited to, Personal Computers, Laptops, Mobile Phones, ipads/Tablets, etc.

GRAHAM are committed to being an inclusive workplace where all employees, customers and stakeholders can fully participate and contribute. We strive to ensure accessibility across all facets of our operations, including physical spaces, digital platforms, communication channels and services.

Our People polices are regularly audited against rigorous accessibility standards to ensure compliance and to support every employee.

Anyone who requires additional support or has any questions regarding accessibility can contact the HR team at HR-JGC@graham.co.uk

2. Remote Working

Remote working is defined as accessing GRAHAM information systems from a place other than a Company office or Site (for example home, client locations, travelling, staff houses, shared accommodation, public areas, etc).

2.1.1. Where possible, a separate room should be used for remote working to avoid accidental disclosure of information to third parties or family members. If a shared space is used, then headphones must be worn when communicating with others online. Care should be taken to avoid shoulder surfing, eavesdropping, etc.

2.1.2. Only secure connections should be used for downloading/uploading information. Wifi networks offered to travellers at airports, hotels, coffee shops and on public transport are insecure and additional measures should be taken to protect and safeguard against information loss.

2.1.3. Only company issued IT equipment should be used to access company information systems. These devices should be logged off and securely stored when unattended.

2.1.4. GRAHAM IT assets (such as laptops, iPads, mobile phones, etc) must not be used by other people (this includes family members).

2.1.5. Only company approved secure online meeting platforms should be used. Particular care should be taken when using online meeting systems to avoid the disclosure of business information either to others in the vicinity of your location or, when allowing the use of shared screens, of information outside the scope of the meeting to other meeting participants.

2.1.6. Hard copies of business information should be securely stored when working remotely until it can be safely returned to the office environment, or confidentially shredded where it is not required to be retained. Care should be taken when printing documents to avoid accidental disclosure/loss. All company information should be returned or confidentially disposed of at the termination of employment.

3. Network Access Requests from outside UK and Ireland

The process relating to network access request is defined within the following sub-sections.

3.1. On Holiday

It is understood that you may wish to keep in contact by email whilst on holiday, but the company would encourage you to enjoy downtime. However, if you do wish to receive emails when abroad on holiday, this should only be via your company issued smartphone, laptops must not be taken abroad. The process to follow:

3.1.1. Discuss with your Division/Function Head for approval

3.1.2. Two weeks prior to your departure, log an IT service request detailing the following:

3.1.2.1. Your holiday destination Country

3.1.2.2. From/To dates

3.1.3. IT will assess the security risk and decide if access can be opened up; your request will either be granted or rejected

3.1.4. A request will be rejected where there is a potential threat to the business. IT will provide an explanation as to the reason for the rejected request

Note: Please do not arrange important virtual meetings that require IT resources when you are away as connectivity is never guaranteed

3.1.5. If your request is granted you must:

3.1.5.1. Always secure your IT devices and ensure they are locked when idle (laptops must not be taken abroad)

3.1.5.2. Use a VPN connection where possible

3.1.5.3. Only accept a MFA (Multi-Factor Authentication) prompt if you are 100% sure you instigated it

3.1.5.4. The IT Acceptable Use Policy must be adhered to at all times

3.2. Working Abroad

Working from a location outside UK and Ireland will only be permitted for a limited period and only in extenuating circumstances such as family bereavement and personal or family illness.

Non-UK/ROI nationals will not be permitted to work from their home country as an extension to a holiday.

Extenuating circumstances will require approval from your Division/Function Head, HR Director and IT Director.

If permission to work abroad is granted, the following rules must be adhered to:

3.2.1. All IT equipment must be kept secure and locked when idle (laptops may only be taken abroad if IT have given approval to do so)

3.2.2. You must use a secure VPN connection

3.2.3. Only accept a MFA (Multi-Factor Authentication) prompt if you are 100% sure you instigated it

3.2.4. The IT Acceptable Use Policy must be adhered to at all times

Note: Please be advised that in the event of a security alert from either the user account or device whilst abroad, access will be cut, and the individual must contact IT immediately. IT Service Desk Support is only available as per the normal UK office hours.

4. Enforcement

GRAHAM reserves the right to audit networks and systems to ensure compliance with Information Security policies. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In situations where non–employees violate this policy, GRAHAM reserves the right to take steps as warranted by the situation, including legal action.

5. Definitions

Term Definition

Remote Working

Remote working is defined as accessing GRAHAM Information Systems from a place other than a Company office or Site (for example home, client locations, travelling, staff houses, public areas, outside UK/Ireland).

6. Associated Policies and Records

IT Acceptable Use Policy