Ixion Group Policy & Procedure

Remote Working

Policy Statement

The Ixion Group (Ixion) provide laptops and other mobile technology to employees who have a business requirement to work away from Ixion premises or who do not have a single secure base from which to work. Other parties are granted permission to access Ixion information remotely to deliver specific services for or on behalf of the company.

Mobile equipment is subject to special security risks: it may be lost or stolen, may be exposed to unauthorised access or tampering. Mobile equipment taken abroad may also be at risk, for example confiscated by police or customs officials. The loss of mobile equipment not only means the loss of the device itself but also of its data, which can lead to the disclosure of sensitive information. This loss of confidentiality, and potential integrity is often more serious than the loss of the physical asset.

Unauthorised access to and tampering with Ixion equipment may:

- lead to continuing (and undetected) compromise of information on the equipment itself;
- undermine security measures (including encryption) intended to protect information in the event of loss or theft; and
- compromise systems to which the equipment is later connected e.g. Ixion networked systems.

Ixion is therefore fully committed to ensuring that employees involved in remote working, and accessing Ixion assets remotely, understand their responsibilities and the procedures they must comply with to attain the same levels of security and data integrity achieved when working directly on Ixion premises.

This policy applies to all employees using company issued mobile equipment and to all parties with remote access to Ixion systems including contractors, services providers and other individuals that process Ixion information in the performance of their duties.

Communication

This policy will be communicated to staff through their initial induction and prior to any equipment or data access being granted for remote working. Contractors or third parties requiring remote access to Ixion systems, will be issued with a copy of this policy to ensure they are fully aware of their responsibilities.

Associated Policies

This Policy and associated procedures should be read in conjunction with the following Policies:

- Information Assurance & Security
- IT User Agreement
- Data Protection
- Lone Working

Definitions

'Remote working' means working outside of Ixion premises and accessing the secure Ixion computing environment from an external location. This may be via a company issued laptop or by other equipment approved by the IT Department.

Authorisation & Issue of Equipment

The use of any information processing equipment outside Ixion premises must be authorised in writing by an employee's line manager or the information asset owner. Regardless of the ownership of the equipment, the use of any equipment processing Ixion information must be authorised by the relevant Director or Head of Department. Where the processing of Ixion client information is proposed on mobile devices, specific written authorisation must be obtained from the information asset owner.

The IT Department will assess risk prior to issuing equipment for remote working, and before granting access to Ixion's network from remote locations, to determine the most appropriate security controls for each individual circumstance.

The installation and configuration of security functionality, including access control, encryption and tamper resistance will be undertaken by the IT Department. This will include, where appropriate:

- FIPS 140-2 full disk encryption for laptops.
- where full disk encryption is not possible, encryption at file or directory level to enable sensitive data to be encrypted whilst at rest.
- BIOS passwords in place that prevent BIOS settings from being changed.
- no facility to boot laptops from external media when in normal use.
- pin or password locks for mobile phones and tablets for the shortest achievable inactivity timeout duration.
- Two-factor authentication to control access to laptops - where this facility is used, the token must not be stored or kept with the mobile device.
- antivirus and security software installed with group policy lockdown of the device and no administrative rights for the end user.
- tamperproof labels fitted to laptops for asset identification, and to disk drives and ports which should not be used.
- implementation of complex password techniques with cryptographic technologies.

All laptops used for Ixion business will be uniquely identified and recorded in the Asset Register by the IT Department. The recipient is fully responsible and accountable for safeguarding the asset, including the data held therein.

Users of laptops and mobile devices will be given appropriate training and instruction in their use and the security functionality and must read and sign the IT User agreement prior to the equipment being deployed. DBS check verification will also be required for the handling of client data.

Data stored on Ixion equipment will be securely erased by the IT Department before being reassigned for another purpose or disposed of when redundant.

Security

Staff working remotely must ensure they work in a secure and authorised manner as set out in the key principles below.

- All contractual obligation; lock down and other good practice security measures to be in effect.
- Passwords must never be kept with the laptop or equipment to which is applies.
- If using equipment in public places, ensure information is not overlooked by unauthorised persons.
- Equipment must not be left unattended in car boots overnight.
- Equipment must not be left unattended in insecure areas e.g. meeting rooms next to areas of public access, and hotel rooms where others may have access. Room locks and lockable storage facilities must be used where available.
- Equipment must not be left in the care of any person who is not trusted to protect the information it contains.
- Staff must be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc. and on public transport.
- When travelling and not in use, ensure laptops are stored securely out of sight.
- When travelling, laptops must not be placed in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots.
- Wifi, Infrared and Bluetooth interfaces should be disabled when not essential by setting their switches to the 'off' position. Users must solely use the wireless software as designated or configured by the IT department.
- Avoid use of unsecured wireless networks to access the internet where possible, if necessary use the Checkpoint VPN connection to access the company resources.
- Laptops with removable media should not be used in places where that media could easily be left behind or misplaced.
- All writable removable media must be encrypted by Checkpoint Endpoint Total Security suite.
- CD/DVD media should not be used if possible and will be disabled by default.
- Where possible laptops should be secured to a desk or other appropriate point if left unattended using an appropriate locking mechanism supplied by the IT Department.

Staff who have been provided with company IT equipment to work remotely must:

- only use this equipment for legitimate business purposes.
- not modify it or attempt to modify it in any way.
- return the equipment at the end of the remote working arrangement or prior to leaving the company.
- not allow non-staff members (including family and friends) to use the equipment.

Sensitive data, including that relating to clients, temporarily stored on an Ixion laptop due to a lack of connection should be kept to the minimum required for its effective business use to minimise the risks and impacts should a breach occur. Data must be transferred to the appropriate central location as soon as possible and removed from the device that the data was captured on.

Loss of Ixion laptops, equipment or data compromise must be reported via the IT Service Desk as per the Information Assurance & Security Policy.

If there is a requirement that quantities of Ixion data are to be held on a single laptop (or any other encrypted storage medium), until they can be transferred back to the appropriate Ixion method of storage for a contract, then a risk assessment as a worst case scenario should consider the impact of loss of all of the data.

Please note that deleted files should be assumed to persist on the laptop's hard disk and therefore IT should be notified for all transfers of equipment before it can be exchanged. Line managers are responsible for keeping equipment untouched in locked storage when equipment is between assigned users that they are responsible for.

Use of Personal Equipment

Personal equipment may only be used within a private environment when absolutely necessary such e.g. invocation of a business continuity facility, special dispensation due to business need. Users who process Ixion information on privately-owned equipment are responsible for the security of the device and must comply with this remote working policy, Ixion's Information Assurance & Security Policy and all contractual obligations as defined from the outset.

Personal equipment must only be used in times of failure of any supplied equipment or special agreement. In these cases, you must access the secure remote Ixion environment using an RDWeb security gateway over https as designated by the ICT department.

No attempt to configure additional access than the above to Ixion data services should be made. No attempt to copy or screenshot any information locally should be attempted. Any attempts to do so could be subject disciplinary proceedings.

Personal mobile phones, tablets or PCs must not be configured in any way by software or app with any access to Ixion systems including email.

Responsibilities

All staff using company issued mobile equipment, or with remote access to Ixion data, are responsible for complying with this policy.

The Head of Service IT is responsible for ensuring full records of all approved remote access working and equipment issued are maintained in accordance with this policy and the Information Assurance & Security Policy. The IT Department will also monitor remote access to Ixion data via system monitoring functionality to ensure the security and integrity of the wider network.

Line Managers, Supply Chain Managers and Human Resources are responsible for:

- correctly authorising remote working;
- notifying the IT Service Desk when this facility is no longer required for an individual member of staff or contractor
- and for monitoring staff to the extent possible, to ensure that all requirements are being met.

Monitoring & Review

The Head of Service IT will monitor requests for remote working, asset register updates, and incident records to assess how effectively this policy is being adhered to. The Head of Service IT will report back at least annually on the effectiveness of the policy and whether any changes are needed.

Ixion reserve the right to monitor and log user account activity, connections to systems and services internally (and externally from Ixion equipment) and to disable access as a precaution when any potential compromise or misuse is suspected for the purposes of Data Protection and Security. This includes but is not limited to URL access, Server access and Database access of which log information may be held in a format and duration in line with Data Protection Law.

On suspected misuse or compromise the ICT department must seek advice from the 'Head of Service – HR' and/or the Registered Data Controller before full investigative powers such as screen viewing or mailbox access can be invoked and all actions taken to must be recorded.

If malware detection systems flag a potential threat, then the remote worker must make their equipment available for inspection and fully comply with all instructions from the ICT department. The ICT Department will endeavour to eliminate any threats immediately and help negate any day-to-day operational disturbances by providing alternative means where possible and creating line manager awareness as necessary.

This policy will be reviewed annually by the Head of Service IT to ensure that it continues to meet current legislative requirements, adopts emerging best practice, and continues to be effective and relevant to the wider business.