CREATIVE
REMOTE

INFORMATION SECURITY POLICY

VERSION 1.2

2024

TABLE OF CONTENTS

CREATIVE
REMOTE

1. General Guidance

- Information Security is everybody's responsibility.
- Creative Remote information systems are provided for business use.
- Use of any Creative Remote Information systems for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this policy.
- Creative Remote reserves the right to monitor any aspect of its information systems in orderto protect its lawful business interests. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings.
- You should have no expectation of privacy when using Creative Remote Information systems.
- Exercise care and common sense in your use of information systems.
- Report any security-related incident to the Management Team.

Breach of this policy will result in disciplinary action. Depending on the severity of the breach, this may include:

- An informal warning from a manager.
- A formal verbal or written warning for misconduct.
- Dismissal for gross misconduct.
- Criminal proceedings.
- Civil proceedings to recover damages.

This policy refers in several places to things that "Others may find offensive". These include but are not limited to:

- Pornographic or sexually explicit material.
- Racist, sexist or homophobic material.
- Tasteless material (such as depiction of injury or animal cruelty).

CREATIVE
REMOTE

2. Communications and Operations Management

2.1 Operational Procedures and Responsibilities

Operating procedures are used in all day to day maintenance of Creative Remote's IT systems and infrastructure in order to ensure the highest possible service from these assets.

Changes to the organisation's operational systems are controlled with a formally documented change control procedure.

The development and test environments must be separate from the live operational environment to reduce the risk of accidental changes or unauthorised access.

Document operating procedures to an appropriate level of detail for the departmental team that will be using them.

Assess all significant changes to the main infrastructure (e.g. Network, Directories) for their impact on

information security as part of the standard risk assessment.

Segregate the development and test environments by the most appropriate controls including, but not limited to, the following:

- Running on separate computers, domains, instances and networks.
- Different usernames and passwords.
- Duties of those able to access and test operational systems.

2.2 System Planning and Acceptance

All Creative Remote IT infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key IT infrastructure components include, but are not restricted to, the following:

- File servers (hosted)
- Domain servers(hosted)
- E-mail servers (hosted)
- Web servers (hosted)
- Printers
- Networks
- Desktops & Laptops

All departments must inform the IT Service Desk of any new product requirements or of any

upgrades, service packs, patches or fixes required to existing systems.

All new products must be approved in writing by the senior management team.

New information systems and product upgrades must all undergo an appropriate level of testing prior to acceptance and release into the live environment.

3rd party applications must also be monitored for service packs and patches.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test

environment that duplicates the operational system.

The acceptance criteria must be clearly identified agreed and documented and should involve

management authorisation.

2.3 Protection against Malicious and Mobile Code

Appropriate steps are taken to protect all Creative Remote IT systems, infrastructure and information against malicious code.

In order to prevent malicious and mobile code, appropriate access controls (e.g. administration / user rights) shall be put in place to prevent installation of software by all users.

Creative Remote staff are responsible for ensuring that they do not introduce malicious code into IT systems.

Where a virus is detected on a Creative Remote system, the individual must inform the IT Service Desk.

Critical security patches must be applied to all software on the organisation network within one month of release and all applicable vendor-supplied security patches are installed within an appropriate time frame.

There must be a full record of which patches have been applied and when.

Requests for software installation shall only be accepted where there is a clear technical verification.

2.4 Backups

Regular backups of essential business information must be taken to ensure that the organisation can

recover from a disaster, media failure or error.

Any 3rd parties that store organisation information must also be required to ensure that the information is backed up.

2.5 Storage Media Handling

Storage media includes, but is not restricted, to the following:

- Computer Hard Drives (both internal and external).
- USB Memory Sticks.
- Digital Cameras.
- Business documentation (company accounts, HR files, etc).
- Backup tapes and magnetic media.

*Creative Remote does not transmit, process or store cardholder information.

Storage media being transported must be protected from unauthorised access, misuse or corruption using an encryption method suitable and effective for the device.

2.6 Documentation

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by any service provider or any other departmental IT staff.

(This does not include generic manuals that have been supplied with software).

Examples of the documentation to be protected include, but are not restricted to, descriptions of:

- Applications
- Processes
- Procedures
- Data structures
- Authorisation details

Effective version control and classification should be applied to all documentation and documentation storage. Storage media that is no longer required is disposed of safely and securely to avoid data leakage.

2.7 Monitoring

As a minimum audit logs must contain the following information:

- System identity
- User ID
- Successful/Unsuccessful login
- Successful/Unsuccessful logoff
- Unauthorised application access
- Changes to system configurations
- Use of privileged accounts (e.g. account management, policy changes, device configuration)

Keep audit logs for a minimum of three months live and twelve months (minimum) archived which record exceptions and other security related events.

Protect access to the logs from unauthorised access that could result in recorded information being altered or deleted. Ensure these logs are stored securely offsite where possible.

Ensure system administrators and users do not erase or deactivate logs of their own activity.

Where appropriate, store classified data separately from non-classified data.

The logs should be checked regularly to ensure that the correct procedures are being followed and reviewed to identify any issues or incidents.

All computer clocks must be synchronised to a reliable time source to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation.#

2.8 Network Management

Network management is critical to the provision of organisation services.

Connections to the network infrastructure must be made in a controlled manner within the office and also within the hosting environment.

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Wireless access SSID (The Collectv U13) is used for business purposes and not used for guest or unauthorised users.

Separate operational responsibility for networks where possible from computer operations activities.

Ensure there are clear responsibilities and procedures for the management of remote equipment and users.

Where appropriate, encryption controls should be put in place to protect data passing over the network

Document the network architecture and store it with configuration settings of all the hardware and software components that make up the network.

Record all components of the network in an asset register.

Ensure all hosts are security hardened to an appropriate level.

Review operating systems network services and disable those services that are not required.

Use encryption on wireless networks to prevent information being intercepted. WPA2 should be applied as a minimum.

All internet connectivity on systems used by Creative Remote's client will be blocked.

Except for specific sites and services which are deemed necessary for the client to perform their role.

In such cases any sites and services are to be approved by Creative Remote on receipt of approval documentation by commissioning companies such as Netflix, Amazon or Apple.

It is the clients responsibility to provide such approvals.

2.9 Systems Development and Maintenance

The General Data Protection Regulation and other legislation applies in this area.

If personal information is used during the development and test phase of preparing application

software it must be protected and controlled in line with the Data Protection Act and where possible depersonalised.

If operational data is used controls must be used including, but not limited to, the following:

- An authorisation process.
- Removal of all operational data from the test system after use.
- Full audit trail of related activities.
- Any personal or confidential information must be protected as if it were live data.

2.10 Annual Health Check

An annual health check of all organisation IT infrastructure systems and facilities should be undertaken by at least every 12 months or following any significant hardware or software change .

This health check must include, but is not restricted to, the following:

- A full penetration test.
- A network summary that will identify all IP addressable devices.
- Network analysis, including exploitable switches and gateways.
- Vulnerability analysis, including patch levels, poor passwords and services used.
- Exploitation analysis.
- A summary report with recommendations for improvement.

3. IT Infrastructure

3.1 Secure Areas

Sensitive information must be stored securely.

A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored. Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted.

The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours
- Window and door locks
- Window bars on lower floor levels
- Access control mechanisms fitted to all accessible doors (where codes are utilised they
- should be regularly changed and known only to those people authorised to access the area/building)
- CCTV cameras

Staff working in secure areas should challenge anyone not known to that individual.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

The Operations Manager must monitor all visitors accessing secure IT areas at all times.

Keys to all secure areas housing IT equipment (i.e. the comms room) and lockable IT cabinets are held centrally by the Operations Manager as appropriate.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach.

Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately.

3.2 Paper and Equipment Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification. If it is classified as sensitive, information security controls to protect it must be put in place.

Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration
- Limit the risk of theft – e.g. if necessary, items such as laptops should be physically attached to the desk
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people

Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure

3.3 Equipment Lifecycle Management

All 3rd party suppliers must ensure that all of Creative Remote's IT equipment is maintained in

accordance with the manufacturer's instructions and with any documented internal procedures to

ensure it remains in working order.

Staff involved with maintenance should:

- Retain all copies of manufacturer's instructions
- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorised technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements
- Record details of faults incurred and actions required

A service history record of equipment should be maintained so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs.

The use of equipment off-site must be formally approved by the user's line manager.

Equipment that is to be reused or disposed of must have all of its data and software erased /destroyed.

If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied:

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded
- Subsequent removal of equipment should be via a formal, auditable process

There should a duty to audit information security arrangements regularly to provide an independent

appraisal and recommend security improvements where necessary.

4. IT Access

4.1 General

All user-level passwords must be changed whenever a system prompts the user to change it.

All passwords are strictly controlled using a secure password manager

Users must not reuse the same password within the last 4 password changes.

All IT systems and procedures will be implemented to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique user name that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.

System administration accounts must only be provided to users that are required to perform system administration tasks.

A request for access to the company's computer systems must first be submitted to the IT Service

Desk for creation. Applications for access must only be submitted if approval has been gained from the user's line manager.

When an employee leaves the company, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the IT Service Desk.

Leaver process includes:

- Revoking access to any restricted areas.
- Revoking access to Windows Domain User Accounts.
- Revoking access to other software portals.
- User's computer/mobile devices are to be handed back along with any peripherals and media.
- The devices should then be securely wiped before being re-issued.

4.2 System and Application Access Control

Access to systems is controlled by a secure login process.

All access to operating systems is via a unique user name that will be audited and can be traced back to each individual user.

The login procedure must also be protected by:

- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.

System administrators must have individual administrator accounts that will be logged and audited.

Access within software applications should be restricted using the security features built into the individual product.

The 'business owner' of the software application is responsible for granting access to the information within the system.

The access must:

- Be compliant with the User Access Management section and the Password section.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

Key systems have Multi Factor Authentication. These include:

- 1 Password.
- DUO MFA admin portal.
- Client virtual machines. DUO MFA.

4.3 Supplier Remote Access

Remote access to Creative Remote's systems by suppliers must be tightly controlled.

Any changes to supplier's connections must be immediately sent to the IT Service Desk so that access can be updated or ceased.

All permissions and access methods must be controlled by the IT Service Desk.

Partners or 3rd party suppliers must have an activity log maintained.

Remote access software must be disabled when not in use.

5. Software

Creative Remote uses software in all aspects of its business to support the work carried out by its employees.

In all instances every piece of software is required to have a licence and the company will not condone the use of any software that does not have a licence.

Software acquisition channels are restricted to ensure that Creative Remote has a complete record of all software that has been purchased for its computers and can register, support, and upgrade such software accordingly.

This includes software that may be downloaded and/or purchased from the Internet. All used software used within Creative Remote is downloaded with an existing license or used as Software as a Service.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software.

All software acquired must be purchased through Creative Remote.

Software must be registered in the name of Creative Remote and the department in which it will be used.

Creative Remote will keep a library of software licenses. The register must contain:

- The title and publisher of the software.
- The date and source of the software acquisition.
- The location of each installation as well as the serial number of the hardware on which each
- copy of the software is installed.
- The existence and location of back-up copies.
- The software product's serial number.
- Details and duration of support arrangements for software upgrades.

Software on Local Area Networks or multiple machines shall only be used in accordance with the licence agreement.

Software must only be installed by Creative Remote once the registration requirements have been met.

All changes to software should be authorised before the change is implemented.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a Creative Remote machine as there is a serious risk of introducing a virus.

Due to project and personnel turnover, software will never be registered in the name of the individual user.

Software must not be changed or altered by any user unless there is a clear business need.

Any Creative Remote user who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under the circumstances. Creative Remote does not condone the illegal duplication of software and will not tolerate it.