Policy Number	**UKCEH/INFOSEC/001**
Policy Author (s)	**Alan Booker, InfoSec Manager**
Policy Approval	**Approved**

Policy Amendment History

Version No.	Date	Amendment Details	Approved By
1	08 2018	Initial Version for G&O	
2	10 2019	Final for UKCEH Go Live	J A Dingle
3	08 2021	Policy rewrite for clarity	Nick Wells

Document Data Classification: Public
Document Audience: All

Contents

1 Purpose

This document forms the **UKCEH Information Security Policy** in support of the **UKCEH Organisational Goals**. Compliance with this Policy will ensure that consistent controls are applied throughout UKCEH to minimise exposure to security, contractual and regulatory breaches.

Failure to protect information assets may lead to costly, time-consuming and damaging incidents and can potentially harm our employees, third parties, our business (including our scientific data and models), and the reputation of UKCEH.

This policy ensures that all employees are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.

Information and information systems are recognised as valuable assets that underpin the strategic goals of UKCEH and so the aim of this policy is to preserve:

Confidentiality: ensuring that information is accessible only to those authorised to have access.

Integrity: safeguarding the accuracy and completeness of information and processing methods.

Availability: ensuring that authorised users have access to information and associated assets when required.

This policy establishes an effective, accountable and transparent framework for managing UKCEH compliance and is aligned with ISO 27001:2013, UK HMG Cyber Essentials and other relevant security standards.

Exceptions to this policy require written approval from the UKCEH Senior Information Risk Owner (SIRO).

2 Scope

This policy applies to the use of information assets and all IT systems, including (but not limited to) laptops, workstations, mobile devices, servers, storage, on premise equipment and cloud based systems which are either used, managed or owned by UKCEH.

Protecting Personally Identifiable Information (PII) and other sensitive and critical scientific and business information will be prioritised.

This policy applies to all staff, students, fellows and temporary staff of UKCEH who have legitimate access to UKCEH information and information assets, technologies and systems. Hereafter referred to as 'employees'.

Where appropriate, this policy also applies to third parties (such as contractors, facility users, collaborators, suppliers and clients) that process, store or transmit UKCEH Data or use/access UKCEH IT Systems. Hereafter referred to as 'third parties'.

This policy applies at locations such as permanent or temporary offices, home/mobile working locations, field sites, institutes, establishments and laboratories operated by UKCEH or wherever information associated with UKCEH is located or accessed from.

3 Information Security Roles and Responsibilities

3.1 All Employees

All employees are responsible for information security and must therefore understand and comply with this policy and associated guidance.

All employees should understand the risks to the information they are processing and how it should be securely handled, stored and transferred.

All employees must report suspected/actual breaches of information security within the organisation.

All employees must undertake their mandatory Data Security Awareness training.

3.2 UKCEH Directors and the Board of Trustees

Responsibility for information security resides ultimately with the Trustees, who delegate responsibility to the UKCEH Executive Board.

UKCEH Directors will ensure that information security management is appropriately coordinated and managed within UKCEH. Directors will ensure that the confidentiality, integrity, availability and regulatory requirements of all UKCEH business systems are met.

3.3 Senior Information Risk Owner (SIRO)

The SIRO shall be the Director of Impact & Innovation and member of the Board and has ultimate responsibility for information risk within UKCEH. The key responsibilities of the SIRO are:

- Ensure that this policy and the information security objectives are compatible with the strategic direction of UKCEH.
- Ensure that data and information assets are identified; that the top level data and information governance roles are allocated and that the post-holders are appropriately briefed on their information security roles and carry out their functions with due diligence.
- Own the risks associated with the information security objectives and ensure that control action owners are identified.

- Ensure that exception procedures are in place to authorise at an appropriate level acceptance or mitigation of significant information security risks that deviate from agreed standards.
- Determine when and by whom, along with the DPO, breaches of information security shall be reported to relevant external authorities.
- Ensure there is clear direction and visible management support for security initiatives and promote continual improvement.
- Ensure the Executive Board and Trustees are adequately briefed on risk management issues.

3.4 Head of IT

The Head of IT is responsible for ensuring that corporate IT assets and services used and/or owned by UKCEH have adequate security measures in place to comply with information security and data protection legislation and regulations. Whilst there are certain agreed technical areas outside the remit of the central IT team (for example application development and field sites), this policy nevertheless applies across the whole organization.

They are the IT subject matter expert and responsible for managing the IT function, including the implementation of new IT systems and policies.

3.5 Information Security Manager

The InfoSec Manager is responsible for developing and implementing the UKCEH Information Security Framework, Policy, Standards, Procedures and Guidance (an Information Security Management System (ISMS)). This will be undertaken in conjunction with the SIRO, the Head of IT, the Data Protection Officer, Information Asset Owners (IAO), owners of other data driven services within UKCEH, and outsourced service providers.

They are the InfoSec subject matter expert and responsible for advising on and promoting all matters InfoSec related, and managing the information security function.

3.6 The Data Protection Officer (DPO)

The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in UKCEH for data protection matters.

They are the DP/GDPR subject matter expert and responsible for promoting and auditing matters DP related, and managing the DP function.

3.7 Information Asset Owners (IAO)

Information Asset Owners are senior individuals involved in running the UKCEH business.

IAOs are responsible for understanding the value, classification, models, access/usage, risks/liabilities, controls, and the lifecycle management (including records) of the data they own.

3.8 Third Parties

Third parties must comply with this UKCEH policy (with equivalent responsibilities to UKCEH employees where appropriate) when accessing or supporting UKCEH systems/network and/or accessing/processing UKCEH data.

Third parties should understand the risks to any UKCEH information they are processing or accessing and how it should be securely handled, stored and transferred.

Third parties must report breaches of information security that occur within their own organization that could materially affect UKCEH.

4 Training, Education & Awareness

UKCEH will ensure annual mandatory information security awareness training, and further guidance at an appropriate level, is given to every individual that has access to UKCEH or client information.

5 Information Risk Management

All information assets will be identified and assigned an Information Asset Owner, who will ensure that information risk assessments are performed annually (or at other intervals where appropriate).

UKCEH will utilise its corporate risk systems to manage, monitor and report on its corporate Information Risks.

UKCEH will continually assess its information risk to assess the level of protection afforded to its information. This will include a threat and impact assessment where necessary.

Risk management, where appropriate, extends to third party suppliers, particularly those supplying hosted information services.

For further details, also read:

- **UKCEH Risk Policy**

6 Acceptable Use

UKCEH IT Systems are for the exclusive use of UKCEH and access to and use of such systems must be limited to UKCEH employees or third parties engaged by UKCEH.

Information and information assets must not be used for inappropriate or illegal purposes

or contrary to their licences.

Employees must comply with all relevant UKCEH policies and procedures, all software licensing agreements, all intellectual property and copyright legislation and all applicable laws and legislation.

Any electronic communication (whether by email, text, or social media or other online forums) must be appropriate.

Employees must not disclose any confidential or commercially sensitive information (including but not limited to scientific, financial, contractual, intellectual property or personal) relating to UKCEH or its clients to any third party without appropriate authorisation.

Employees must not transfer files and documents to or from non UKCEH IT systems unless there is a valid business case to do so.

Employees must not introduce unauthorised data to a UKCEH IT system or inappropriately delete, copy, download or extract UKCEH information.

Employees must not store, create, download, access or pass on any text, image, graphic or other material which could be regarded as inappropriate, offensive, illegal or discriminatory on the grounds of race, sex, sexual orientation, religion, belief, age or disability.

For further details, also read:

- **UKCEH Acceptable Use of ICT Systems and Services Policy**
- **UKCEH Social Media Policy**

7 Monitoring of Activity

UKCEH reserve the right to monitor, record, intercept, block and access IT Systems and electronic communications including emails, social media, mobiles, network access, remote access and web usage for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- Ascertaining compliance with regulatory or self-regulatory practices or procedures

For further details, also read:

- **UKCEH Acceptable Use of ICT Systems and Services Policy**

8 Information Records/Asset Management

All records/assets created, received, maintained, held, archived or potentially destroyed, in any format or media type, by UKCEH employees in the course of carrying out their work, must be managed in accordance with the UKCEH Records Management and UKCEH Data Protection policies, and in line with legal and business requirements.

All records/assets should have an identified owner responsible for their management whilst in regular use, and for appropriate retention and disposal. This person or role is defined as the Information Asset Owner (IAO).

Based on confidentiality requirements, information should be classified against one of the four UKCEH Data Classification categories - Public, Internal Use, Restricted or Confidential.

All UKCEH data assets, and where appropriate client's assets, must be protected using appropriate and proportionate mechanisms (typically encryption and/or access control) both in transit and at rest, as per the UKCEH Data Security Policy.

An information asset register will be maintained showing all important data assets, including PII. Acceptable use of such assets will be included, as will the “risk appetite”.

For further details, also read:

- **UKCEH Data Encryption Standards**
- **UKCEH Data Protection Policy**
- **UKCEH Data Security Policy**
- **UKCEH Data Classification Policy**
- **UKCEH Records Management Policy**
- **UKCEH Records Management Process**

9 Protection from Malicious Software

UKCEH have in place extensive systems to minimise the likelihood of malicious software. These include perimeter firewalls, web and email filtering, application control, endpoint detection and response, and advanced persistent threat detection. However, several additional precautions should be taken by UKCEH employees:

- Do not open any emails, including attachments, from unknown or suspicious sources. If in doubt please ask the IT Help Desk before opening.
- Unapproved software must not be introduced and run on UKCEH systems without the permission of the IT/InfoSec departments. Consideration will be based on the business case, alternatives, cost, integration and support requirements, and security.
- Treat with suspicion any removable media such as USB devices from external sources. If the media is from an unknown source, do not connect it to UKCEH devices or the network. The IT Help Desk must be informed immediately if a virus alert is triggered.

- Beware of unexpected phone calls, especially if passwords, account details, or other personal or business sensitive information is requested. If in doubt please contact the IT Help Desk.

10 Removable Media

Removable media containing UKCEH or client data must be encrypted where possible as per the UKCEH Data Encryption Standards and the UKCEH Data Security Policy

For further details, also read:

- **UKCEH Data Encryption Standards**
- **UKCEH Data Security Policy**

11 System and Data Access Control

All UKCEH systems, including but not limited to mobile, tablet, laptop, desktop, workstation, server, network, appliances and cloud utilize controlled access by means of unique user credentials including passwords. Additionally Multi-Factor Authentication is deployed across the UKCEH estate.

Access to systems and specific data sets shall be restricted by role to users who have an authorised business need to access the information and as approved by the relevant IAO.

Users will be given the minimum access to sensitive information or key operational services necessary for their role.

Privileged Access Rights shall be restricted and tightly controlled. This shall be documented.

Access by third parties must be authorized and agreed by the IAO, IT and InfoSec. This shall be documented.

Access will be removed when individuals leave their role or the organisation. Periodic reviews should also take place to ensure appropriate access is maintained.

UKCEH will manage devices which have access to sensitive information, or key operational services, such that technical policies can be applied and controls can be exerted over software that interacts with sensitive information.

UKCEH will ensure appropriate and proportionate physical security measures are in place to safeguard information and information assets.

For further details, also read:

- **UKCEH Password Policy**
- **UKCEH Physical Security Policy**
- **UKCEH IT Operations Policy**

12 Systems Acquisition and Disposal

UKCEH's Procurement Policy is to use preferred and framework suppliers. Where no preferred supplier is available for the proposed IT hardware, software or system, IT and InfoSec will be involved in the review and approval process at an early stage of the on-boarding.

Employees must submit requests for hardware, software, systems or services (including cloud services such as SaaS, PaaS or IaaS) to IT. Consideration of non-standard/unapproved hardware, software or systems will be subject to a rigorous appraisal and testing procedure based on the business case, possible alternatives, cost, integration and support requirements, testing, and security.

Business requirements must take into account the security architecture principles of security by design, defence in depth, least privilege, default deny and fail secure.

Only hardware and software approved by the IT Department and appropriately licensed can be connected to or accessed via the UKCEH IT infrastructure.

New apps, websites, data portals or APIs ("Digital Properties") must be approved by the Head of Communications and Engagement, Head of Applications Development, or if unavailable, another member of the Web Governance Board.

New project websites will normally be built within the ceh.ac.uk domain. However, where a new domain outside ceh.ac.uk is required, a business case must be approved by the Head of Communications & Engagement or the Head of Applications Development.

Details of digital properties must be maintained up to date within the Digital Properties Catalogue.

The IT Department maintains the software asset register along with all software licenses and media.

All disposal of IT equipment must be conducted via IT to ensure that it is done securely and that any information remaining on any storage device is securely wiped.

For further details, also read:

- **UKCEH Procurement Policy**
- **UKCEH Purchasing of IT Equipment Policy**
- **UKCEH Web Services Policy**
- **UKCEH IT Equipment and Data Disposal Policy**

13 Business Continuity and Disaster Recovery

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2019).

Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The Board has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

For further details, also read:

- **UKCEH Business Continuity Strategy**
- **UKCEH Business Continuity Plan**
- **UKCEH Incident Response Plan**

14 Patching

UKCEH will develop, maintain, deploy and monitor system patch status as detailed in the UKCEH Lifecycle, Patch Management and Code of Connection Policy.

All employees must allow software updates and patches that the IT department deploy, to proceed in a timely fashion.

Applications and systems that are End of Life (EOL) and for which security patches are no longer available, must be retired. If for significant business reasons they need to remain in production, mitigating controls must be deployed (such as removing them from the UKCEH network) and this must be agreed at Board level.

For further details, also read:

- **UKCEH Lifecycle, Patch Management and Code of Connection Policy**

15 Information Security Incident Reporting/Response

All actual, near miss, or suspected information security incidents must be reported immediately using the UKCEH Information Security Incident Reporting System (CISIR). Examples of incidents include malware outbreaks, attempted or known hacking, data breach or suspected breach, loss of a mobile device, and theft of a laptop or memory stick.

Employees must report to the IT Help Desk in a timely manner any actual or suspected security weaknesses in UKCEH IT systems or third-party systems/services used by UKCEH, so that they can be investigated and addressed.

UKCEH will handle any data security incidents with the same extremely high priority as any other business continuity incident.

UKCEH will have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services. This will ensure the continuity of key operational services in the event of failure or compromise.

For further details, also read:

- **UKCEH Information Security Incident and Event Process**
- **UKCEH Data Protection Policy**

16 Information Security Design Principles

UKCEH will adhere to a core set of design principles when designing and implementing information systems. When one or more of these principles cannot be applied for business or technical reasons, and this leaves the information asset unduly exposed and at unacceptable risk, acceptable mitigation/compensating mechanisms must be deployed.

Secure by Design - on the commencement of an IT or Data project or programme, a risk assessment must be carried out, which considers security, privacy and other risks.

Segregation of Duties - conflicting duties and areas of responsibility will be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of UKCEH assets.

Least Privilege - employees will only be given those access privileges which are essential to perform their role.

Secure by Default - when new software and systems are introduced, they will be configured before going into production so that the default configuration is secure, for example access will have to be explicitly granted.

Segmentation of Network - UKCEH will maintain segmentation of the internal network to limit potential attack surfaces, by the use of VLANs or other appropriate controls.

17 IT Change Control

Changes to IT systems including off-the-shelf software and networks shall be controlled. This will involve a review/approval process by IT, Information Security, and where applicable other stakeholders such as the business owner.

18 Data Protection

UKCEH holds and processes personal data about individuals defined as ‘data subjects’ by the law. Such data must only be processed in accordance with the GDPR and the DPA.

UKCEH has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with the GDPR and the DPA.

All users of personal data within UKCEH must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally.

Loss or suspected loss/leakage of UKCEH or client data, especially when this is Personally Identifiable Information (PII), must reported to the UKCEH DPO immediately.

For further details, also read:

- **UKCEH Data Protection Policy**

19 Contracts of Employment

Employee contracts of employment must contain an appropriate confidentiality clause.

The Employee Handbook shall contain appropriate Confidentiality and Computer, Internet and Email Use clauses outlining expectations of employees.

20 Suppliers and Third Parties

Third parties (such as suppliers and clients) that process, store or transmit UKCEH Data or use UKCEH IT Systems must comply with this policy unless explicitly directed otherwise.

Access to UKCEH systems and information by third parties must only be granted where there is a strong business case to do so. A suitable risk assessment should be undertaken and approval must be given in writing by the IAO/business owner, IT, InfoSec, and where PII is involved, by the DPO. InfoSec expectations must be clearly communicated to, and agreed by, third parties for example by the use of Letters of Appointment, Service Level Agreements, Contracts, Non-Disclosure Agreements, Data Sharing Agreements and similar documentation.

Third parties that process/store information on behalf of UKCEH cannot share that data with any other body without prior approval from UKCEH except where required by UK law.

IAOs are responsible for ensuring appropriate data protection / security assurance from third party suppliers processing/storing UKCEH data.

Employees must not pass on confidential UKCEH data to suppliers or other third-parties without authorization by the relevant IAO.

21 Remote Access and Travelling

UKCEH information that is held or processed on systems outside of UKCEH premises is generally more exposed to being compromised, corrupted or lost than information that is

held or processed on systems within UKCEH premises. Additional precautions/controls must therefore be applied based on the identified risk factors.

All employees must ensure they protect UKCEH equipment and data assets when operating remotely, whether that is from their own residence or when travelling further afield.

Employees are responsible for ensuring that they connect to the UKCEH network via the VPN at least weekly to ensure new software patches and security configurations can be applied.

Employees must complete the UKCEH Authorisation for Overseas Travel Form when travelling abroad and if the risk rating is deemed medium or higher, complete the UKCEH Overseas Risk Assessment form. Based on this, employees must seek advice from IT as special precautions must be adhered to, for example, temporary devices may be assigned and remote access prohibited.

The loss of any UKCEH device, especially one which contains UKCEH or client data, must be reported to IT immediately.

A breach or suspected data breach when remote, especially if PII related, must reported to the UKCEH DPO immediately.

For further details, also read:

- **UKCEH Remote, Overseas and Mobile Policy**
- **UKCEH Travelling with IT and Risk Destinations Policy**

22 Bring Your Own Device

Only UKCEH equipment can directly access the 'core' IT systems, services, and network.

Access via a browser to Microsoft 365 including Outlook is allowed, though Multi Factor Authentication (MFA) will be enabled.

BYOD access is permissible for employees using the 'Eduroam' or 'UKCEH-Visitor' Wi-Fi systems.

For further details, also read:

- **UKCEH Bring Your Own Device Policy**

23 Review of this Policy

This policy will be reviewed at least annually, or more frequently as required.

24 Core Supporting Documents

- UKCEH Acceptable Use of ICT Systems and Services Policy
- UKCEH Bring Your Own Device Policy
- UKCEH Business Continuity Plan
- UKCEH Business Continuity Strategy
- UKCEH Data Encryption Standards
- UKCEH Data Protection Policy
- UKCEH Data Security Policy
- UKCEH Data Classification Policy
- UKCEH Incident Response Plan
- UKCEH Information Security Incident and Event Process
- UKCEH IT Equipment and Data Disposal Policy
- UKCEH Lifecycle, Patch Management and Code of Connection Policy
- UKCEH Passwords Policy
- UKCEH Physical Security Policy
- UKCEH Procurement Policy
- UKCEH Purchasing of IT Equipment Policy
- UKCEH Records Management Policy
- UKCEH Records Management Process
- UKCEH Remote, Overseas and Mobile Policy
- UKCEH Risk Policy
- UKCEH Social Media Policy
- UKCEH Travelling with IT and Risk Destinations Policy
- UKCEH Web Services Policy

End of Document