Security Policy

Version: 016

Classification: Commercial in Confidence

KCOM is the trading name of KCOM Group Limited and its subsidiary companies.
Registered office 37 Carr Lane, Hull, HU1 3RE
Registered number 2150618

KCOM

Business Areas affected by this Policy: All

Definitions of Terms Used:

Definitions of Terms Used:	
Asset	Anything that has value to KCOM
Contractor	Any person who is employed by an external organisation who provides goods and/or services directly to KCOM.
Customer	A person or organisation that KCOM provides a product or service to.
Employee	Any person who is employed by KCOM
Secure Area	A physical area in which access is restricted to authorised people, such as Data Centres etc.
Supplier	Any person, partner or organisation involved in supplying goods or services to KCOM.
Subcontractor	Any person who is employed by an external organisation who provides goods and/or services indirectly to KCOM.
Third Party	Any 'Supplier','Customer' or 'Contractor'

KCOM

Contents

1 Policy Statement....5
2 Reason for Policy....6
3 Our Security Objectives....7
4 Responsibilities....7
4.1 Chief Executive Officer (CEO)....7
4.2 Executive Leadership Team (ELT)....7
4.3 Chief Technology Officer (CTO)....8
4.4 Transformation Portfolio Director....8
4.5 Head of Risk and Compliance....8
4.6 Senior Information Risk Owner (SIRO)....8
4.7 Information Risk/Asset Owner....8
4.8 People Managers....8
4.9 Employees and Contractors....9
5 Employee Security....9
5.1 Contract of Employment....9
5.2 Termination or Change of Employment....9
6 Information Security Awareness, Education and Training....9
7 Remote working....10
7.1 Mobile and Portable Devices....10
8 Physical and Environmental Security....10
8.1 Physical Perimeter Controls....10
8.2 Physical Entry Controls....10
8.3 Protection against Physical and Environmental Threats....10
8.4 Working in Secure Areas....11
8.5 Equipment Security....11
8.5.1 Equipment Siting and Protection....11
8.5.2 Equipment Maintenance....11
8.5.3 Supporting Utilities....11
8.5.4 Cabling Security....11
8.5.5 Removal of Property....11
8.5.6 Security of assets off-premises....12
8.5.7 Secure disposal or re-use of Equipment....12
8.6 Clear Desk and Clear Screen Policy....12
9 Risk Management....12
10 Asset Management....12
11 Information Governance....13
11.1 Classification of Information....13
11.2 Handling Guidelines....13
11.3 Information Transfer....13
12 Data Protection....13
13 Supply Chain Management....13
14 Identity and Access Control....14

15 Operational Management 14
15.1 Operational Procedures 15
15.2 Change Management 16
15.3 Network Security Management 16
15.4 New, development and maintenance of systems, networks, products and services 16
16 Encryption 17
17 Security Incident Management 17
17.1 Reporting Security Incidents 17
18 Business Continuity and Disaster Recovery 17
19 Contact with authorities and special interest groups 17
20 Legal, Statutory, Regulatory and Contractual Requirements 18
20.1 Applicable legislation, regulations and standards 18
21 Sanctions 18
22 Exceptions 18
23 Related Policies, Processes and Procedures 19
24 Contacts 19
25 Review Arrangements 19
26 Summary of Changes 19

1 Policy Statement

KCOM is one of the longest-established providers of communications services in the UK, connecting both businesses and residential customers and investing in better digital solutions for everyone.

We recognise the importance of maintaining the **confidentiality**, **integrity** and **availability** of its information and its customers' information, and to protect its people, properties and assets.

To achieve this, KCOM's Information Security Management System provides a framework to implement and monitor the governance, risk management and compliance of organisational, people, physical and technological controls across the business, in accordance with applicable legislation, regulations and industry standards and best practice.

Tim Shaw
Chief Executive Officer

KCOM

2 Reason for Policy

The purpose of this Security Policy ("Policy") is to:

- Establish, implement, maintain and continually improve KCOM's information security management system
- Communicate the security objectives and requirements to maintain KCOM's information security management system
- Protect KCOM's information and assets from all threats, whether internal or external, deliberate or accidental and to preserve its confidentiality, integrity and availability
- Provide assurance to interested parties such as customers regulatory bodies and employees that the confidentiality, availability and integrity of their information will be maintained appropriately
- Ensure that information security requirements are identified and addressed in all projects and strategic decisions
- Minimise the business impact from security risks and threats.

This Policy applies to all assets that must be protected from potential or actual threats, including systems, networks, applications, locations, people and customer assets.

KCOM is certified to the ISO/IEC 27001:2022 Information Security Management System standard and the scope of the certification is as follows:

Information security management system for the delivery of communications and associated technologies, products and services. The scope also covers the supporting functions within Group Services and activities carried out at Data Centres and Switch Sites in the UK. This is in accordance with the KCOM Statement of Applicability.

KCOM

3 Our Security Objectives

The following objectives have been agreed in order to evaluate the performance and effectiveness of the information security management system:

1. Promote a positive and pro-active cyber security awareness culture
2. Build and maintain secure and resilient networks and systems
3. Meet our relevant security legal, regulatory and ISO/industry standards requirements
4. Adopt a pro-active approach to managing emerging threats and vulnerabilities.

4 Responsibilities

4.1 Chief Executive Officer (CEO)

The CEO has ultimate responsibility at board level for security and provides support to embed security into KCOM and developing a positive security culture.

4.2 Executive Leadership Team (ELT)

The ELT are responsible for supporting the information security management framework and for ensuring their business area complies with this Policy and related procedures.

Their responsibilities include:

- ensuring that information security objectives are integrated into processes;
- providing clear direction and visible management support of the security objectives;
- supporting plans and programmes to promote and maintain information and physical security education, training and awareness;
- providing input to the direction and progress of security to ensure its continuing suitability, adequacy and effectiveness;
- ensuring an asset register is maintained in their business area;
- ensuring that information security risks are assessed and mitigated to an acceptable level;
- implementing effective security measures and controls;
- ensuring risk assessments are carried out on critical assets and that they are reviewed annually, or sooner if there is a significant change to the asset;
- ensuring Risk Registers are maintained in their business area;
- planning and responding to security incidents;
- ensuring all security incidents and risks identified in their business area are reported; and providing a point of escalation for any security risks, incidents and audit findings.

4.3 Chief Technology Officer (CTO)

The CTO is KCOM's Executive Leadership Team member responsible for implementing appropriate physical and cyber security controls to protect KCOM's sites, networks and systems and permitter edge for Corporate IT network.

4.4 Transformation Portfolio Director

The Transformation Portfolio Director is responsible for implementing appropriate cyber security controls to protect KCOM's Corporate IT systems.

4.5 Head of Risk and Compliance

The Head of Risk and Compliance is responsible for implementing and maintaining the information security governance (including data protection), risk management and compliance framework and will:

- develop and review the relevant policies and associated procedures, and ensure that information security is integrated with other KCOM policies;
- develop and maintain an information security (including cyber security and data protection) strategy and programme;
- implement and maintain an information security management framework;
- ensure information security and privacy risks are managed in accordance with KCOM's Risk Management framework;
- provide cyber security training and awareness across KCOM.
- ensure compliance with this Policy is monitored and continually improved.

4.6 Senior Information Risk Owner (SIRO)

The SIRO is the ELT of the business area that is providing the product or service and is responsible for the risk profile of the product or service, ensuring all risks have been identified and appropriate mitigations are in place so that risks can be accepted.

4.7 Information Risk/Asset Owner

The role of an Information Risk or Asset Owner is to understand the purpose and what information is being, processed stored, how it is handled and who has access to it, in order to assess and address the risks.

4.8 People Managers

People Managers are responsible for ensuring that the Employees and Contractors working within their area are aware of this Policy and any applicable related policies and procedures, and to ensure that appropriate security controls are implemented and maintained.

They must ensure that Employees and Contractors (who have direct corporate access to networks and systems) within their area complete the relevant security awareness training appropriate to their role and that records are maintained.

4.9 Employees and Contractors

All employees and contractors are responsible for complying with the requirements of this Policy and any applicable related policies and procedures.

Any employee who is responsible for managing the relationship or is the point of contact for a Third Party must ensure that the requirements of this Policy and any applicable related policies and procedures are followed.

All employees responsible for any security related procedures must ensure that they comply with this Policy, any legal requirements and relevant standards to avoid breaches of any law, statutory, regulatory or contractual obligations.

5 Employee Security

5.1 Contract of Employment

Security roles and responsibilities must be defined and clearly communicated to all potential employees and Contractors prior to commencing work for KCOM in accordance with the Recruitment and Selection Policy and contractual requirements.

Background verification checks on all potential employees, contractors and suppliers (if applicable) must be carried out in accordance with the Security Screening Policy and contractual requirements.

5.2 Termination or Change of Employment

It is the responsibility of the People Manager to promptly forward details of any leaver or role changes to the HR Operations team, and where applicable, retrieve all company assets in a timely manner. People Managers are also responsible for completing the Leaver Checklist in accordance with the Leaver Procedure.

6 Information Security Awareness, Education and Training

Mandatory cyber security awareness training is provided as part of KCOM's induction process and annually as refresher training, and must be completed by all employees. Additional security related training is provided to relevant employees and contractors (where applicable) as required by their roles and responsibilities.

KCOM

7 Remote working

All Employees and Contractors must maintain the same level of security controls as in the office, such as working from home or at an off-site location.

7.1 Mobile and Portable Devices

All employees and contractors must comply with the requirements of the Mobile and Portable Devices Policy to ensure the security and proper use of company mobile and portable devices.

8 Physical and Environmental Security

All employees must comply with the requirements of the Physical Access Procedure, including wearing their security ID card at all times on KCOM sites, in order to prevent any unauthorised physical access, damage or interference to KCOM properties, assets and information.

It is the responsibility of employees managing relationships with or Suppliers or Contractors to ensure that they are made aware of and comply with the Physical Access Procedure, and that they are requested to report any actual or potential physical security incident in accordance with KCOM's Security Incident Management Procedure.

In order to prevent unauthorised access, destruction, damage or interference to KCOM physical and information assets, the following controls must be applied:

8.1 Physical Perimeter Controls

Perimeter controls must be established in accordance with the appropriate level of risk and may include intruder detection systems, CCTV, manned receptions, fencing etc.

Signage on buildings must be appropriate to their level of risk, as detailed below:

- Offices must have appropriate external signage
- Switch Sites, Data Centres and BNAPs must give minimum indication of their purpose or use.

8.2 Physical Entry Controls

Documented procedures must detail the appropriate levels of control to ensure access is limited to authorised people only, including third party access rights.

Public access to KCOM's assets must be restricted at all times. Where public access is necessary or unavoidable, appropriate controls must be implemented.

8.3 Protection against Physical and Environmental Threats

There must be appropriate protection against physical and environmental threats such as:

- Fire
- Flood
- Explosive and asphyxiating gases

- Civil unrest etc.

The appropriate level will be determined by carrying out the relevant risk assessments.

8.4 Working in Secure Areas

Any person working in a secure area without appropriate authorisation must be supervised at all times.

Procedures and arrangements should be in place and communicated, to prevent any safety and security related incidents within a secure area.

8.5 Equipment Security

To minimise loss of or damage to assets, the following controls must be applied to protect the relevant equipment:

8.5.1 Equipment Siting and Protection

All equipment must be stored, positioned and protected to prevent any physical loss, damage, theft or compromise of the asset.

Equipment must be protected from potential physical and environmental threats such as theft, fire, dust, communication interference etc. and any other disruption caused by the failure of supporting utilities.

8.5.2 Equipment Maintenance

Equipment must be maintained in line with manufacturer's recommendations and maintenance records must be kept.

8.5.3 Supporting Utilities

Supporting utilities such as electricity, water, air conditioning etc. should be maintained and regularly inspected and tested.

Where necessary, generators or uninterrupted power supplies must be installed and maintained to prevent the loss of service.

Where generators are provided, adequate fuel (normally 72 hours running time) must be available and checked regularly.

8.5.4 Cabling Security

Any power or telecommunications cabling must be protected from any interference or physical damage that may affect the operation of the equipment it supports.

8.5.5 Removal of Property

No equipment, information or software should be removed from KCOM sites without permission.

In certain circumstances, KCOM may introduce random searches of vehicles, people or equipment.

8.5.6 Security of assets off-premises

All KCOM equipment installed on a Third Party site must be protected from any physical and environmental threats and have adequate security controls to prevent unauthorised access.

8.5.7 Secure disposal or re-use of Equipment

All items of equipment containing storage media must be disposed of in accordance with their contractual requirement or as detailed in the Waste Arrangements.

8.6 Clear Desk and Clear Screen Policy

A clear desk policy must be maintained, such that customer and other confidential information is not left on desks, and computer screens must not be left unlocked whilst unattended.

9 Risk Management

Information Risk/Asset Owners are responsible for ensuring security and privacy risks are identified and assessed on all assets such as buildings, products, services, systems, data and processes to ensure that appropriate technical and organisational controls are in place.

The security risk assessment and privacy impact assessment must be carried out in accordance with the Security and Privacy Risk Assessment Procedure.

10 Asset Management

All assets that are valuable to the KCOM must be identified on an asset register. Each asset register must be owned, regularly reviewed and maintained.

The asset register must contain a description of the asset and a designated ‘Asset owner’. The Asset Owner is responsible for controlling the production, development, maintenance, use and security of the assets.

The term ‘Asset Owner’ does not mean that the person actually has property rights to the asset.

All areas responsible for managing assets must ensure that it has an acceptable use policy for the use of its assets and that this is communicated to the relevant users.

All assets must be returned to the relevant asset owner upon the termination of a contract or employment.

KCOM

11 Information Governance

11.1 Classification of Information

Appropriate classification controls must be applied to all KCOM information and must represent its value, legal requirements, sensitivity and criticality to the business.

The information classifications are defined in the Data Governance Policy.

11.2 Handling Guidelines

The requirements of the Data Governance Policy must be followed for the handling, storage and disposal of data.

11.3 Information Transfer

The requirements of the Data Governance Policy must be followed when sending or sharing information.

Confidential or Non Disclosure Agreements (NDA) must be in place to protect the transfer of any confidential information between parties, except where it is required for regulatory or legislative reasons (in which case, the Legal team must be consulted).

12 Data Protection

KCOM takes data privacy and data protection seriously. To ensure that it meets its obligations to keep the personal data it holds about its customers and its employees secure, it has a policy that sets out the framework for ensuring accountability and governance in relation to data protection.

Refer to the Data Protection Policy for details.

13 Supply Chain Management

Contractual agreements with a supplier must be in place setting out the appropriate information or physical security requirements prior to the delivery or use of any product or service.

It is the responsibility of the supplier to notify KCOM as soon as they become aware of any changes (including starters, movers and leavers) that impact the logical or physical access to KCOM information systems or property, to ensure that the appropriate KCOM assets are assigned or retrieved and access is updated or removed.

All areas responsible for managing relationships with suppliers providing a service delivery function must ensure that the appropriate security controls, service definitions and delivery levels are implemented, operated and maintained by the supplier.

The services provided must be monitored, reviewed and follow the appropriate change management process.

All suppliers must comply with the Supplier and Partner Code of Conduct, and any specific security requirements such as training and awareness, security screening, right to audit etc. included in the

supplier contract. All security obligations must flow down the supply chain to maintain the level of security.

Refer to the Procurement and Vendor Management Policy for details.

14 Identity and Access Control

All areas responsible for managing access to physical or information assets such as locations, systems, networks etc. must have a documented procedure covering the following controls relevant to their area:

- Access control, including:
  - formal authorisation of access requests;
  - periodic reviews of access rights;
  - removal of access rights.
- User access management such as granting, revoking or changes to access rights, privilege management, user password management and review of user access rights.
- User responsibilities such as password use and unattended user equipment.
- System and application access control, covering:
  - restriction to information and application systems, and the isolation of confidential data, applications or systems;
  - secure log on procedures;
  - password management in accordance to the Password Policy Guide;
  - the use of utility programs such as anti-virus software.;
  - restriction of access to program source code.

15 Operational Management

All areas responsible for the operational management of information assets must ensure that the following controls are managed and controlled effectively:

- Segregation of duties and responsibilities are applied (where necessary), to reduce opportunities from unauthorised or unintentional modification or misuse of the KCOM's assets, and to ensure an authorised individual cannot disable an entire operational network, either maliciously or accidentally.
- Separation of environments such as development, test and operational environments are used to reduce the risks of network traversal and unauthorised access or changes to operational systems.

- Capacity management planning must be carried out to ensure continued system performance and that no external parties can overload the network. The performance of systems, networks and resources must be proactively monitored.

- System acceptance procedures and tests must be carried out on new, and updates to, information systems, applications and networks prior to their release in an operational environment.

- Back-up copies of information and software must be taken and an offline copy securely maintained and tested regularly in accordance with the agreed backup procedures.

- Protection against malware such as the detection, prevention and recovery controls and, if appropriate, procedures, must be implemented to protect KCOM's assets from the threat of malware.

- Logging and monitoring of events such as user and system administrator activities, exceptions and information security events on networks and systems must be produced and retained. This must be carried out in accordance with the Logging and Monitoring Policy Guide.

  If system logs are not produced automatically, the change management process must record or log any system activity.

- Clocks must be synchronised to the Coordinated Universal Time (UTC) such as GPS or UK National Physical Laboratory to ensure that the time and date of activities are recorded accurately.

- Installation or use of software must be controlled and not installed on KCOM equipment without appropriate authorisation.

- Vulnerability and patch management must be carried out to prevent the exploitation of vulnerabilities. Any vulnerabilities identified must be addressed, or security controls put in place within the relevant timescales set out in the Vulnerability and Patch Management Policy Guide.

- Security testing and vulnerability scanning activities must be planned and agreed to minimise the impact on operational systems.

15.1 Operational Procedures

All areas responsible for the operational maintenance of information systems must ensure that operating procedures are documented, maintained and available to all users who need them, and include:

- Security related aspects such as change management, configuration of network elements, operational support systems and vulnerability management;
- Description of the nature of security testing to be carried out before deployment into an operational system;
- Equipment maintenance and safety;
- Instructions for the detailed execution of each job, including scheduling requirements, interdependencies with other systems, the management of audit trails and system log

information.

15.2 Change Management

All areas responsible for carrying out changes to information systems, applications and networks must have a documented change management process to ensure all changes are controlled, tested and appropriately approved. Records of the tests carried out, the results and approvals must be maintained.

15.3 Network Security Management

Networks must be managed and controlled to ensure that information is protected, and the availability and integrity of the network is not affected.

All areas responsible for the management of networks must ensure that procedures and controls are in place, to ensure the security of the information in the network and the protection of its connected services from unauthorised access.

Where applicable, network service agreements must be in place detailing the relevant security arrangements such as security features, service levels and management requirements.

15.4 New, development and maintenance of systems, networks, products and services

All areas responsible for implementing new, or developing and maintaining existing systems, networks, products or services must ensure that security requirements are considered, and that an appropriate security risk assessment is conducted.

Any technical vulnerabilities identified must be addressed, or security controls put in place to prevent errors, loss, unauthorised access, modification or misuse of information. If applicable, a security plan must be developed.

The security of applications connected to, and integrity of information made available on, public networks such as the internet must be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

The following controls must be applied to ensure that the relevant security requirements are achieved and maintained:

- Change Management, such that:
    - changes must follow the appropriate change control procedures;
    - technical reviews and tests of critical applications are carried out;
    - changes or modifications are appropriately controlled.
- Secure Environments established for all environments including development, test and operational.
- Outsourced development is reviewed and tested.
- Testing of any security functionality.

Test data must be protected at all times to prevent unauthorised access. The use of test data containing personally identifiable or confidential information must be avoided, and if it is not possible, all confidential details and content must be removed or modified.

16 Encryption

Data such as personal data must be encrypted to help secure it both in transit such as email, memory sticks etc. and at rest such as stored on laptops, servers etc.

Refer to the Encryption Policy Guide for details.

17 Security Incident Management

All security incidents, weaknesses or threats must be reported as soon as we become aware of them, to enable immediate corrective and/or preventative action to be taken and notification to the relevant party within the required notification period.

Refer to the Security Incident Management Procedure for details.

17.1 Reporting Security Incidents

All employees and contractors must report any potential or actual security incident or data breaches using the Security Incident Reporting Form KCOM Incident Management - Power Apps.

Any third party employee must report any actual or potential security incident or data breach to their relevant KCOM point of contact.

18 Business Continuity and Disaster Recovery

It is important to ensure that KCOM's networks and systems are resilient and business continuity and disaster recovery plans are in place to prevent business disruption.

Refer to the Business Continuity Policy for details.

19 Contact with authorities and special interest groups

KCOM will maintain effective communications with relevant organisations providing security advice, so that we remain aware of any security threats and vulnerabilities.

Any employee who has any formal contact with government or security agencies must notify the Head of Risk and Compliance or email risk@kcom.com.

KCOM

20 Legal, Statutory, Regulatory and Contractual Requirements

20.1 Applicable legislation, regulations and standards

KCOM has a responsibility to comply with applicable legal, statutory, regulatory and contractual requirements, such as:

- Anti-terrorism, Crime and Security Act 2001
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1998
- Cyber Essentials and Cyber Essentials Plus
- Data Protection Act 2018 and UK General Data Protection Regulations
- Data Retention (EC Directive) Regulations 2009
- Electronic Communication (Security Measures) Regulation 2022
- Investigatory Powers Act 2016
- Minimum Security Standards for Interconnecting Providers (NICC ND 1643)
- NCSC Cloud Security Principles
- NCSC Cyber Assessment Framework (CAF)
- Network and Information Systems Regulations 2018
- NHS Data Security and Protection Toolkit
- Official Secrets Act 1989
- Payment Services Directive (PSD2)
- Payment Card Industry Data Security Standards (PCI DSS)
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000, Chapter 23
- Section 105 A-D of the Communications Act 2003 (security requirements)
- Telecoms Security Act 2021

This is not an exhaustive list.

21 Sanctions

Failure to comply with this Policy and supporting policies, standards and procedures is a disciplinary offence. The severity of any disciplinary action will reflect the potential risk to the business, its assets or reputation. Serious breach of this Policy may result in dismissal or prosecution. All action will follow the Disciplinary Procedure.

Refer to the Exceptions section of this Policy for any exemption.

22 Exceptions

Where the control requirements defined in this Policy cannot be met, a security risk assessment must be carried out and any risks appropriately mitigated.

KCOM

23 Related Policies, Processes and Procedures

- Business Continuity Policy
- Data Governance Policy
- Data Protection Policy
- Disciplinary Procedure
- Encryption Policy Guide
- Leaver Procedure
- Logging and Monitoring Policy Guide
- Mobile and Portable Devices Policy
- Non Disclosure Agreements
- Password Policy Guide
- Physical Access Procedure
- Procurement and Vendor Management Policy
- Recruitment and Selection Policy
- Security Incident Management Procedure
- Security and Privacy Risk Assessment Procedure
- Security Screening Policy
- Supplier and Partner Code of Conduct
- Statement of Applicability
- Vulnerability and Patch Management Policy Guide
- Waste Arrangements.

24 Contacts

For further information and guidance on this Policy, contact the Head of Risk and Compliance or email risk@kcom.com.

25 Review Arrangements

This policy will be reviewed at least annually or sooner if required by the Head of Risk and Compliance.

26 Summary of Changes

Version	Changes	Final Approval	Date Approved
016	• Responsibilities section updated in line with organisational changes • Applicable legislation, regulations and standards updated	CEO	26/03/24
015	• Objectives updated in line with business strategic focus. • Responsibilities section updated in line with organisational changes.	CEO	12/12/23