Information Technology Management Policy

Purpose and Audience

Purpose: To set the expectations of necessary and appropriate management of Information Technology (IT) to ensure its effective, safe and compliant use across the University in support of all the strategic priorities; education, research and engagement. This policy includes details of expected IT management outcomes, and associated responsibilities and accountabilities.

Audience: This policy applies all those in academic divisions and professional services who manage IT Services of all levels of complexity across the whole University or in localised areas, devolved areas or departments.

Definitions

IT Service

An IT service encapsulates the provision, management and use of IT equipment or systems to provide a university (academic, teaching, research, professional service, engagement) outcome for a user or group of users. Included are those owned by the University and those leased, rented or otherwise contracted facility where the University has control.

Roles

User - A 'user' as defined in the Full IT Regulations, with no elevated privileges. This policy is largely not relevant to such a user, who is guided by the Full IT Regulations.

Privileged user - A user with additional responsibilities for or access to an IT service, but short of system administrator. Often in the role as a senior operator or team specialist or service champion or reporting officer or subject expert.

System Administrator - The person with the duty to control the operation or the use of the IT Service. The staff and contractors who have responsibility to operate or control IT systems, or networks or significant portions thereof. This includes similar role titles, such as Network Manager, Database Administrator, Web Master, Domain Administrator, System root, etc.

Line Manager - In this context the line management of system administrators or privileged users. A line manager is not necessarily a systems administrator or privileged user themselves, but in the larger IT teams they are.

Business systems owner - The accountable person (or their delegate) for an IT Service, who defines the business requirement, secures or allocates resources to provide the IT Service, and accounts for its delivery.

Governance - Any group, committee or board that wholly or in part that is the accountable body for an IT service.

Tenets of IT Services at Kent:

We use the following tenets of good IT Service management to guide us. Our IT services will be:

EFFECTIVE

- Usable – appropriate OS, software, compute power,
- Reliable – warranty, support (break/fix), backups
- Maintained –updates, upgrades, lifecycle (refresh etc)

SAFE

- Secure in terms of IT Security; Confidentiality, Accuracy, and Availability
- Physically secure (I.e. Prevent theft, appropriate to the system)
- Safe to use – e.g. electrically safe - following Safety, Health and Environment Unit & Estates guidance.

COMPLIANT

- Compliant with English and Welsh Law (including but not limited to Computer Misuse Act, Data Protection Act, The Public Sector Bodies Accessibility Regulations 2018)
- Licences and all necessary contractual terms
- Meets the University Procurement regulations

Policy

This document is divided into the following sections to organise the IT management into coherent interrelated blocks. These are guided by advice from the National Cyber Security Centre (NCSC).

1. Operations Management
2. Identity and Access Management
3. Systems Management
4. Network Management
5. Software Management
6. Vulnerability Management (including patching & updates)
7. Data Custodianship
8. Monitoring and Logging
9. Systems Administrator Authority

1. Operations Management

This section outlines the requirements for the implementation and maintenance of a secure, resilient and safe operational environment. This applies to all IT owned or operated by the University.

- Proportional measures based on a risk assessment of the environment must be taken to protect IT systems against accidental damage, security breaches, theft, or malicious intent. This can include but not limited to a locked dedicated space, secure cabinets, etc
- Data centre areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control, as determined with advice from University Security, Insurance, Information Services and Information Compliance teams as appropriate. Staff which are authorised to enter such areas are to be provided with information on the potential security risks and the measures used to control them.
- The procedures for the operation and administration of all systems and activities forming part of or related to the University's information systems must be documented by those responsible for them, these procedures and documents shall be reviewed at appropriate intervals.
- Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have management approval.
- Duties and areas of responsibility shall be appropriately segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University.
- Development and testing facilities for business-critical systems shall be logically separate from operational facilities and the migration of change from development to operational status shall be subject to IT Services change process.
- Acceptance criteria for new IT Services, upgrades and new versions shall be established and suitable tests of the systems carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of data are in place.
- Assets of the University including IT hardware need to be recorded and the record maintained as required by the University Financial Regulations, or delegations as appropriate.
- System Administrators need to clarify with their Line Managers and relevant Business Systems Owners the existence of and familiarity with business continuity plans.

- Business Systems Owners need to ensure business continuity plans include consideration for IT services and that regular training and testing includes Systems Administrators
- All IT services operating for the University (on premise or remote) to be documented within the central Information Services IT Service Catalogue
- System Administrators must track the lifetime of systems and services as advised by manufacturers and suppliers. Plans for dealing with end of life must be timely and coordinated with the Business Systems Owner in terms of resource planning.
- All end of life plans must address timely removal of obsolete systems, suitable transfer or preservation or deletion of data in accordance with data retention and records management policies.

2. Identity and Access Management

It is vital the University controls who and what can access the University's IT services, systems and data. Understanding who or what needs access, and under what conditions, is just as important as knowing who needs to be kept out. The central identity and access management system is the primary system to achieve this. Application of Single Sign On to all systems should be the aim as this give the best and most effective experience for the Users along with appropriate consistent control by the University.

- All IT Services should use the central Single Sign On (SSO) service. Where this is not possible exceptions can be made but only with the explicit recorded permission of IS. The accountability burden must then be carried by the exceptional system's System Administrator and Line Manager of operating an additional authentication system, and steps should be taken to move the exceptional system to the central SSO as soon as practicable.
- The student record and HR systems are authoritative sources for valid users. Any exceptions for creating users from outside of these processes must be justified and recorded. The authoritative sources define joiners and leavers. Any exceptions to this must be handled with care and be appropriately robust and accountable.
- The user life-cycle providing one or more IT accounts and related access permissions needs to be clearly defined to include joining, role changes within life-cycle, and departure. Inaction in respect of an account should lead in defined time frames to automatic removal of all permissions and eventual retirement of the account. There are processes for identifying and maintaining exceptionally long duration accounts and permissions.
- Assignment of access permissions should be automated and based on data held within the authoritative sources or derived from downstream systems. Ad hoc assignment of permissions should be avoided, and where used suitably recorded.

- Multi factor authentication must be used for all access to IT services requiring authentication.
- All authentication credentials must be adequately protected both at rest and in transit. Any written record of a password must be secure, passwords can be stored in appropriately protected password manager programs.
- IT service or system accounts with administrative privileges should be separate from the System Administrator normal user account. Access to administrative level, should be only when necessary (e.g. via SUDO). On campus MFA should be considered for highly privileged accounts.
- System Administrators should review user accounts and systems for unnecessary privileges on a regular basis, and ensure privileged accesses are revoked when no longer required.
- No account should be shared between multiple users. Where this is absolutely necessary its existence needs explicit recording and additional controls put in place to ensure accountability for system administration, e.g. access restricted via a jump server.
- Cached passwords should be avoided, persistent inter-systems connections should be secured by key exchange or other suitable method.
- Authentication and authorisation events (successes and failures) must be logged and monitored for indications of potential compromise.

3. Systems Management

This section covers all the IT Systems owned or operated by the University and any computers that are present on the campus network which are connected under the agreed Business and Community Engagement Jisc Policies. It is vital that such resources are properly controlled, maintained and managed.

- The University’s Information Systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve data security, confidentiality and integrity.
- All systems management staff must have up to date Information Security and GDPR training, and retake this training at suitable regular intervals.
- System Administrators responsible for Information Systems are to maintain the appropriate access controls for their systems and keep records of any elevated access they give to users.
- System Administrators or individuals responsible for Information Systems are responsible for correct and secure operation of computers in accordance with related University policies.

- Access to all Information Systems, excluding publicly accessible data sources, shall use a secure authentication process. Consideration should also be given as to whether it is appropriate and feasible to further limit or control the access to business critical systems. Access to information systems is to be logged and monitored where appropriate.
- System Administrators and individuals responsible for the Information Systems must ensure that appropriate backup and system recovery procedures are in place, dependent upon the assessed level of criticality of the information concerned. Backup of the University's information systems and critical assets and the ability to recover then is an important priority. Recovery from backup should be regularly tested.
- System Administrators should, where appropriate and feasible, include resilience and redundancy features. These need to be regularly tested to confirm they function as designed and suitable records kept of the test result.
- System Administrators are responsible for ensuring that the University's information systems and critical data is frequently backed up and procedures for recovery meet the needs of the business.
- Only authorised staff will be permitted to perform systems administration functions. Use of commands to perform these functions should be logged and monitored where it is considered appropriate and feasible to do so.
- Formal change control procedures, with audit trails, shall be used for all changes to business critical systems. All such changes must be risk assessed and authorised by the IT Services Change Advisory Board or relevant line manager before being moved to the live environment
- In advance of any substantial change to system(s) or their connection to the IT infrastructure or network System Administrators should discuss the proposed changes with the relevant technical owners of affected service, or if in doubt contact Information Services.
- Systems connected to the network should have appropriate configuration and controls, such as firewalls, to defend the system from inappropriate access. Only required services should be offered by the system.
- Remote access to services should be appropriately secure, controlled, authenticated (inc MFA) and accounted for by design and not rely on additional measures such as VPN.
- System clocks must all be synchronised to the University's NTP service. In the case of computers in the Active Directory this will happen automatically.

4. Network Management

This section refers to the University network, including the wireless network. The University network covers all building on all campuses. It includes student halls of residence on the Canterbury campus. Also covered is the protection of networked services to ensure that users who access the network and networked services do not compromise the security of these services.

- Information Services is responsible for the effective, safe and compliant operation of the network. All connections to the network must be compliant with relevant standards and required configurations. Delegated network segments must be designed and operated with the performance of the overall network taking precedence.
- The University network shall be managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security and integrity. All network management staff shall be given relevant training in information security.
- The network must be designed and configured to deliver levels of performance, security and reliability suitable for the University’s business needs, whilst providing a suitable degree of access control.
- Information Services is responsible for providing the enterprise wireless network service. Devolved areas or Professional Services are prohibited from establishing their own wireless network or adding wireless access points unless specifically authorised to do so. The frequency spectrum is a precious resource and its use must be optimised for the best experience of students, staff and visitors.
- The network should be segregated where appropriate into separate logical subnetworks taking into account security requirements. Appropriately configured firewalls and other security mechanisms where appropriate shall be used to protect the sub-networks supporting the University’s business critical systems.
- The network should where appropriate and feasible include resilience and redundancy features. These need to be regularly tested to confirm they function as designed and suitable records kept of the test result.
- New networks or changes to network designs need to be done under the control and authority of Information Services. This applies to new building or building refurbishment or substantial change of use.
- Other IT Specialists may undertake network moves if relevant training and an agreement with Information Services is in place.
- Switch based reconfigurations of a users’ network will only be carried out by staff from the within Information Services or with specific delegations to authorised Systems Administrators.

- The implementation of new equipment or upgrades to network software or firmware must be carefully planned tested and managed.
- The Change Advisory Board must approve any changes.
- AAA (triple A) (authentication, authorisation and accounting) methodology must be implemented on network devices wherever possible using technologies such as RADIUS and TACAS+. All network appliances will have their management interfaces appropriately secured and controlled.
- Where there is a risk of the network security, quality of service for network users, or in order to enforce University policy, System Administrators are authorised to proportionately:
    - Impose restrictions on network traffic or use of network applications;
    - Refuse connection of devices to the network;
    - Remove networked devices or sub-sections of the network from service;
    - Manage network resource allocation (e.g. bandwidth).
- Information Services are authoritative for the domain name space and the IP address space (including all public and all private address spaces) and the routing design. Portions may be delegated as appropriate. The whole space and all delegations must be managed and records maintained.
- All IP address assignments are temporary. Systems Administrator cannot assume that long duration assignments are an indication of permanency. Integrated assignments (e.g. system IP and related firewall) are controlled and managed on a case by case basis.
- Information Services are authoritative for the network time service. All systems connected to the network must consume reliable time synchronisation from NTP or Active Directory as appropriate.
- Remote access to University IT Services are normally secured within the service themselves by modern industry standard components (inc. MFA SSO). However, to accommodate the business variety of systems Information Services provides an SSO MFA protected VPN service; when remote ‘tunnelled’ access is unavoidable the central VPN service is the only acceptable means of remote ‘tunnelled’ access.

5. Software Management

Provision and use of software is important for proper conducting of University business. The University must meet its legal, including copyright, obligations for the use and distribution of software, whether the software is charged for or otherwise is free of financial cost.

- Systems Administrators and Line Managers need to be able to account to governance bodies ensuring that all software used within the University, and stored on computers for which the Systems Administrators is responsible for has been properly obtained and is being used within the terms of the software licence.
- Due to requirements placed on the University to monitor and report on software installations and use, from time to time the University will be subject to audit, all IT service owners and systems administrators must proactively support such audit activities.
- Software found that is not licence compliant must be brought into compliance promptly or uninstalled
- Information Services have an established collection of software applications covering a broad range of University functions and requirements, before considering procuring new or different software Line Managers should consider whether the requirement can be met from existing available software.
- Software must be purchased in accordance with university purchasing procedures ensuring that the correct type and number of licenses are being purchased.
- When staff or students leave the University, any University software entitlements for software installed on computers they own cease, so all such software must be immediately removed.
- Software must be maintained and kept secure. There must be procedures for deploying new versions and patches to all instances of the software.
- When decommissioning a computer system for disposal or re-use, appropriate measures must be taken in relation to any software and data stored on it.
- The design and development of bespoke software and applications should be undertaken with due consideration for the commitment to support the software over time and the compliance obligations that may arise. Commensurate with the risk to the University of the software Systems Administrators should obtain agreement of Line Managers or Governance. Advice of Information Services can be sought.
- Business Systems Owners should adjust business processes to fit standard software configurations available from the suppliers as a priority over creating bespoke code to support unique University business practices. This minimises cost and risk.

6. Vulnerability Management

This section addressed the requirement to keep the University IT Services secure from malicious attackers, but also the necessary and appropriate maintenance and updating of IT Services. The majority of cyber security incidents are the result of attackers exploiting publicly disclosed vulnerabilities to gain access to systems and networks. Attackers will, often indiscriminately, seek to exploit vulnerabilities as soon as they have been disclosed. It is important (and essential for any systems that are exploitable from the internet) to install security updates as soon as possible to protect the University and the data we are custodians of. Some vulnerabilities may be harder to fix or to fix quickly, the vulnerability management process will help prioritising which ones are most serious and need addressing first, and which alternative proportionate mitigations are appropriate.

- Systems Administrators and Line Managers must establish and maintain vulnerability management process for the systems they are responsible for, alongside methods to track and confirm patch deployments. This needs to include processes to gain up-to-date understanding of vulnerabilities so they can be addressed promptly, and necessary work planned.
- Systems Administrators must use automated patch and update deployment services where available and appropriate.
- Limit the impact of problematic updates by test staging, staggering updates and have a rollback strategy available.
- For compliance reasons the aim should be to deploy critical security related updates / patches within 14 calendar days of release by manufacturer.
- Systems Administrators should triage vulnerabilities to have a clear idea of the severity, risk of exploitation and the impact, and decide which ones need fixing based on business risk. Refer to the vendor’s vulnerability advisory information as this will be the most accurate and up-to-date.
- Prioritise fixing vulnerabilities and put in place alternative mitigations for those which are more difficult to fix. Consider the risk of exploitation alongside the costs and practicalities of mitigating them. Ensure any unmitigated vulnerabilities are well-managed, and resultant risks captured in a risk register.
- Devices should have appropriate anti-virus and anti-malware solutions installed on them. This software must be kept up-to-date and its operation should not be suspended. Logs and alerts from such software need to have proportionate review.
- IT services should be configured to deliver secure by default operation.
- Information Services is the primary liaison route with Jisc csirt, and the National Cyber Security Centre (NCSC). All System Administrators and Line Managers must promptly assist Information Services in any request for assistance or information.

- All equipment and software must be supported by the manufacturer or supplier. When this ceases the item in question is considered beyond end of life and its replacement or removal from service should be addressed without delay.
- If one component of a system is obsolete, always continue to update and patch the other components of the system, where possible.
- Systems which are obsolete or beyond end of life or unsupported by the manufacturer but nonetheless are essential to the University and are otherwise unable to be replaced must be specifically protected, associated risks mitigated, and such actions explicitly recorded in the service catalogue. The Business Systems Owner must seek replacement at the earliest practicable opportunity.

7. Data Custodianship

The University depends on data collected and managed effectively through the many university (academic, teaching, research, professional service, engagement) processes, this data and the information therein is valuable and must be used as effectively as possible. The University data needs to be protected in transit, at rest, and at end of life from unauthorised access, modification, or deletion in accordance with relevant data retention or records management policy. Overall the lead on managing information is led by the Directorate of Governance and Assurance, this section addresses the issue for a Systems Administrator. The data protection act requires Appropriate technical and organisational measures must be used to protect personal data.

- Systems Administrators need to clarify with Line Managers or Business systems owners the nature of the data being held or processed by the IT system.
- Business systems owners are responsible for defining the need for collecting, creating, storing, processing, sharing and deleting data of the University. The timeliness of the steps in this process are important, and where possible Systems Administrators should look to automate the activities.
- Systems Administrators working with Business systems owners need to support the effective, efficient, and secure sharing of data between systems. The aim should be to maintain single authoritative sources of truth whilst maximising the use of the data and supporting effective and efficient maintenance of the data in an accountable way.
- Systems Administrators should avoid storing unnecessary data, and consolidate data where possible to make it easier to secure and manage. Where there is a requirement for data to be replicated or cached, ensure that all copies are sufficiently protected and similarly controlled.
- Ensure that data is appropriately protected in transit to ensure data is not inappropriately viewed or interfered with. For example all web sites must be protected by up to date encryption with publicly issued certificates.

- Ensure that data is protected at rest. Implement physical and logical access controls so that only authorised users can access and/or modify your data. Disk encryption should be used where there is a risk of physical theft, e.g. data held outside of central data centres.
- All portable devices must be encrypted.
- Use current standardised cryptographic algorithms to protect your data. Old algorithms or those that haven't been accepted as standards will provide less protection and could result in a false sense of security. Ensure where cryptography is used, protect the cryptographic material (such as certificates and keys) from unauthorised access.
- Ensure interfaces that enable access to sensitive data are well defined and expose only the necessary functionality to reduce the opportunity for an attacker to abuse them. Access to bulk datasets should be carefully controlled. Only grant the ability to run arbitrary queries over sensitive datasets to users if there is a legitimate business need and it's carefully monitored. This should be considered a privileged role.
- Systems Administrators should ensure that an offline or immutable backup is kept separate from the system, if in doubt consult Information Services. The backups must be protected from unauthorised access, modification, or deletion to the same degree as the primary.
- Backups must be tested regularly.
- Reduce the risk of re-infection when restoring data from backups by re-installing executables from trusted sources instead of backup, and ensuring operating systems and application software is up to date on the target systems. Malware may persist in backups, so you should ensure files are scanned using up to date antivirus software when they are being restored.
- Systems Administrators must have a rigorous process to ensure end of life storage media is sanitised before disposal. This can be by means of a robust contract with a suitable third party. Consider periodic verification that data is being sanitised as described, and test destruction processes and equipment.

8. Monitoring and Logging

Monitoring and collecting logs from IT Services are one of the most useful tools in detecting and investigating problems with IT systems and services. Logs can provide information about system faults and misuse as well as early warnings of problems. Monitoring involves the active analysis of logging information to look for signs of known attacks or unusual system behaviour, enabling the detection of events or statuses that are a risk to or detrimental to the University.

- There are a number of legal issues that must be addressed in any logging activity. Even if the logs contain only information that the network was used by particular accounts, then they will constitute personal data within the meaning of the Data Protection Act 2018 (particularly the Privacy and Electronic Communications (EC Directive) Regulations 2003).
- This places restrictions on how logs may be used, and also requires that they be protected against misuse by appropriate technical and procedural measures. Personal data may only be kept so long as there is good reason to do so: organisations should ensure that they have a retention policy stating how long logs will be held and that they are deleted after this period.
- If the logs contain the content of any communication, for example the text of e-mails, news or chatroom conversations, then recording them counts as interception and the conditions of the Investigatory Powers Act 2016 must also be met.
- System Administrators should implement logging and monitoring that is proportionate to the context of the system, the threat that the University faces and the resources available.
- System Administrators should log accesses to data and monitor for unusual queries, attempted bulk exports of data, and administrative access to detect possible compromises.
- System Administrators should consider where to store logs. Discuss with Information Services whether central or local storage is most appropriate. Central storage will allow for analysis across data sets. If sending logs to a central log service, use transport encryption and one-way flow control where appropriate.
- System Administrators should ensure the reliability of log services. Alerts which are acted on when logging deviates from designed processes.
- Protect logs from tampering so that is it hard for an attacker to hide their tracks and you can be confident that they accurately represent what has happened.
- Where monitoring shows evidence of a service problem the System Administrator will be notified in order to take remedial action. If the fault is affecting secondary systems or services Information Services will take appropriate action to best protect the University and its business processes. Where malicious activity is suspected this will be reported to appropriate authorities, and proportionate protective action taken.
- All IT systems, devices and networks will be regularly scanned and tested for vulnerabilities. Where a vulnerability or security breach is detected, action will be taken immediately to ensure the security of the wider University interests. This will include, but not limited to, the complete shutdown of the service and suspension of access regardless of service impact.

9. Systems Administrator Authority

Systems administrators and privileged users need to perform actions which may result in the disclosure of information held by other users in their files, or sent by users over communications networks. Systems Administrators also perform other activities, such as disabling machines or their network connections, that have no privacy implications. They do so under the delegated authority of the Director of Information Services, "the person with a right to control the operation or the use of the system".

- If any Systems Administrator or privileged user is ever unsure about the authority they are working under then they should stop and seek advice immediately, as otherwise there is a risk that their actions may be in breach of the law.
- Systems Administrators or privileged user must always be aware that the privileges they are granted place them in a position of considerable trust. Any breach of that trust, by misusing privileges or failing to maintain a high professional standard, not only makes their suitability for the system administration or privileged user role doubtful, but is likely to be considered by their employers as gross misconduct.
- Systems administrators and privileged users must always work within Kent's policies, and should seek at all time to follow professional codes of behaviour such as the British Computer Society (BCP) Code of Conduct and Code of Good Practice (https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf)
- If during the course of their duties they discover misuse this must be appropriately reported.
- Systems Administrators' responsibilities are divided into types of activities; Operational, and Policy.

Operational:

- The first duty of a Systems Administrators is to ensure that systems, services and networks are available to users and that information is processed and transferred correctly, preserving its integrity.
- Systems Administrators can where necessary to ensure the proper operation of systems or services for which they are responsible;
- examine any relevant files on those computers
- monitor and record traffic on those networks or display it in an appropriate form
- rename any relevant files on those computers or change their access permissions (see Modification of Data below)
- create relevant new files on those computers

- The Systems Administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

Policy:

- Systems Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users both that such monitoring will be carried out and the policies to which it will apply. Or specific permission has been provided.

Disclosure and Modification of Data

- Systems Administrators are required to respect the secrecy of files and correspondence. During the course of their activities, Systems Administrators are likely to become aware of information which is held by, or concerns, other users. Any information obtained must be treated as confidential - it must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation:
- Systems Administrators must be aware of the need to protect the privacy of personal data and sensitive personal data (within the meaning of the Data Protection Act 2018) that is stored on their systems. Such data may become known to them during the course of their legitimate work. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the relevant data controller.
- For both operational and policy reasons, it may be necessary for Systems Administrators to make changes to user files on computers for which they are responsible. Wherever possible this should be done in such a way that the information in the files is preserved.
- Systems Administrators must be aware of the unintended changes that their activities may make to systems and files. And take steps to prevent or mitigate unintended changes.

Document review date

This policy will be reviewed annually by ISC.

Policy created: 06/2022

Policy reviewed: 07/2023