Ulster University Code of Practice Cover Sheet

Document Title	IT Monitoring Code of Practice 1.6
Custodian	Deputy Director of Finance and Information Services (Information Services)
Approving Committee	ISD Committee
Policy approved date	2017 – 08 – 10
Policy effective from date	2017 – 08 – 10
Policy review date	2018 – 08 – 10

Changes to previous version

Page 6 – Added “, Network Access Control (NAC)”

INFORMATION TECHNOLOGY (IT) MONITORING POLICY – IT MONITORING CODE OF PRACTICE

Related Documents

1. JISC Legal Information - Interception and Monitoring of Communications in FE and HE 2006 http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/esecOverview.pdf
2. The Regulation of Investigatory Powers Act 2000 ('the RIPA')
3. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

Scope

The scope of this standard applies to all staff and students of the University.

Purpose

The University operates its Information and communications equipment, networks and systems (including Telephony) as private systems for the use of its staff, associates, visitors and students. The University has the right, responsibility and the necessity, to oversee and control the operation and use of its Information Technology. The purpose of this document is to define codes of practice for the monitoring of University Information Technology, and for the interception of communications; in order that such monitoring is carried our lawfully and that appropriate governance and oversight is applied.

The Code of Practice

Monitoring Information Technology

Monitoring shall be conducted in accordance with the Regulation of Investigatory Powers Act 2000 and under lawful business practice. It shall be proportionate to achieving its purpose and respecting the privacy of individuals. Monitoring, scanning and interception of data shall only be performed by authorized personnel, and may be performed without consent. Monitoring will normally be carried out by staff in the designated role of a) IT Systems Manager and/or administrator and b) Network Managers. Monitoring will normally be performed by these authorized staff on the systems and networks for which they are the designated manager.

The use of University networks, systems and services shall be monitored by authorised personnel for the following general purposes:

- To ascertain compliance with legislation, regulations, University Policy and Codes of Practice;
- To ensure acceptable use;
- To assure confidentiality (security), integrity and availability:
    - Investigate or detect unauthorized use of the Information Technology;
    - To assist in fault investigation and incident handling;
    - To facilitate capacity planning and optimize performance;
    - Ensure the efficient and effective operation of the system.
- Prevent or detect crime;
- Ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system;

Monitoring but not recording is also permissible in the following cases:

- To ascertain whether the use or communication is business or personal;
- To protect or support help-line, service desk or technical support staff.

Resultant logs shall be retained or archived for an agreed period (ref: University Retention and Disposal schedule) so that they are available to be studied in the

event of a problem or security incident, and to ensure that users are only performing processes that have been explicitly authorized.

Users of the University Information Technology shall be notified that monitoring takes place.

Monitoring shall not be conducted for the purposes of establishing performance or efficiency of employees (except where local agreements have been made with staff).

Authorised Personnel

Senior Officers of the University may authorise their staff to conduct Information Technology monitoring and shall keep a register of authorized persons and the networks and systems which they are authorized to monitor. Such persons will normally be network and system managers and/or administrators. System administrators may only monitor systems for which they have direct responsibility or authorization for. Authorized personnel shall execute their duties in accordance with the Systems Administrators Code of Practice. In particular authorised personnel must:

- Respect the privacy of others;
- Not use or disclose information realised in the monitoring process for purposes other than those for which the process was approved;
- Safeguard information collected in the monitoring process;
- Destroy information collected in the monitoring process when it is no longer required;

Monitored Information

Information, which is the result of monitoring, may be used to assure acceptable use, compliance with University Policy, and may be the subject of investigative requests by University authorities, law enforcement and other external agencies. Requests for Monitoring information from external agencies shall be submitted in writing, for approval, to the Deputy Director of Finance and Information Services (Information Services).

Information obtained in the course of monitoring may be disclosed to the following:

- The Department of Health, Social Services and Public Safety (or any successor body);
- Any professional body in conjunction with whom or on whose behalf Ulster University conducts courses;
- Such other external organizations or persons as Ulster University may consider appropriate having regard to the nature of a particular breach of University Policy.
- Law enforcement agencies
  All requests from LEAs shall be submitted formally on the form – “Request for Disclosure of Personal Data”. Informal requests from external agencies will not be accepted or processed.

Monitored information includes, but is not limited to, the following:

Network, System or Service	**Monitored Information**
Telephones	The use of telephone systems in terms of date, time, duration, call destination/origination and cost.
Internet access and Web content monitoring	Internet access using University information and communications equipment and telephony is checked for key "danger" words, or destination addresses which would suggest the access is for an inappropriate or illegal purpose. The discovery of any such words can lead to an escalation of monitoring and/or automatic referral to the Police Service of Northern Ireland. Software may be used to monitor the use of certain sites and the nature and volume of downloaded materials
E-Mail	Incoming E-Mail shall be filtered for Spam. For reasons of business continuity, E-Mails are stored, archived and are discoverable through search and/or browsing by authorized staff.
Network usage	Network statistics – peak and average bandwidth utilization and errors. Unusual network traffic.
Servers	CPU utilization and active processes. File storage utilization, anomalies, file types and file

	sizes. System and security log anomalies
Authentication	Successful authentication attempts – user account, date/time stamp and session duration. IP address tied to specific workstation. Unsuccessful access attempts.
Software licensing	Software download, installation and use.

Log Descriptions

Monitored logs include, but are not limited to, the following:

Log	**Log Description**
Routers and firewalls	Routers can export network flow records, which normally need processing to extract useful information, to a collector system. They can also keep records of packets matching access control lists. Whilst continuous logging of all traffic is recommended, often a specific access control list can be useful in answering a question. For instance, it would be possible to log all attempts to send e-mail directly from client computers, in support of a policy that they should not do so. Where a VPN (Virtual Private Network) is implemented in a router or firewall, the device can capture records of use, attempted use and authentication.
E-mail gateways	The header of an outgoing e-mail message usually includes enough information to trace the message back to a particular workstation in the network, and combined with authentication and access logs, to an individual user. While it may be desirable for some header information to be excluded from outgoing E-Mails, the information shall still be logged.
DHCP servers	DHCP logging must be enabled on DHCP servers to allow DHCP leases to be matched to workstation physical MAC addresses.
Authentication and access servers	It is essential that there is a record of who was logged in to any workstation at any time. Typically the records will be generated by an authentication, login, Network Access Control (NAC) or RADIUS server.
NAT	Any NAT device (Network Address Translation) should log each

gateways	new translation, so that given the public IP address in your network, source port for some traffic flow, and the time, you can recover the internal source IP for that traffic.
Proxy servers	For the same reasons as NAT, Web proxies should log each URL with the time and the internal IP address requesting it, so that any request can be traced to its source. Logging is likely to be complementary to that from NAT gateways. Similar considerations apply to proxies for other kinds of service.
Network Access	Many sites are now using Network Access Control technologies to authenticate network layer access to their networks. Records of authentication can be very useful in tracing use of both wired and wireless public networks back to an individual rather than a specific workstation or laptop.

Clock Synchronization

The correct setting of real time clocks on computers is essential to ensure the accuracy of audit logs, which may be required when investigating a problem or as evidence in legal or disciplinary cases. It is important that the correct time zone and daylight saving setting are configured.

The University maintains authoritative synchronized time sources. Currently, the primary time source for networks, systems and services within the University are the major backbone routers which synchronize with JANET via NTP. ISD administered lab, staff and student workstations registered on the University's Active Directory domains are synchronized with the authoritative University time source. Faculty and departmental network, systems and services shall also be synchronised with the authoritative University time source listed below,

clockc.ulster.ac.uk – Coleraine Campus

clockj.ulster.ac.uk – Jordanstown and Belfast Campus

clockm.ulster.ac.uk – Magee Campus

Log Retention Schedule

Log files are one of the most useful tools in detecting and investigating problems with computer systems. Logs can provide information about system faults and misuse as well as early warnings of problems. System administrators should therefore log key activities and refer to these logs when troubleshooting problems or investigating misuse. JANET currently recommends retaining logs for up to 12

months for subscriber data, 6 months for most traffic data and 4 days for web cache data.

The University maintains a Retention and Disposal Schedule, and retention and disposal schedules for logfiles shall be included in the schedule.

Monitoring Notification

When authenticating and connecting to University networks, systems or services, users shall be informed that monitoring is being conducted as follows:

In the course of normal business, the use of University networks, systems and services is logged and interactively monitored by authorised personnel for the following general purposes:

- ***To ascertain compliance with legislation, regulations, University Policy and Codes of Practice;***
- ***To ensure acceptable use;***
- ***To assure confidentiality, integrity and availability:***
    - ***Investigate or detect unauthorised use of the Information Technology;***
    - ***To assist in fault investigation and incident handling;***
    - ***To facilitate capacity planning and optimise performance;***
    - ***Ensure the efficient and effective operation of the system.***
- ***Prevent or detect crime;***
- ***To gather evidence for investigative or disciplinary purposes;***
- ***Ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.***

Monitoring is conducted in accordance with the Regulation of Investigatory Powers Act 2000 and under lawful business practice shall be proportionate to achieving its purpose and respecting the privacy of individuals.

Requests for Monitored Information

All requests for information obtained by IT monitoring shall be submitted to the Deputy Director of Finance and Information Services (Information Services)

Directed Investigation

Any request to authorised personnel to conduct detailed monitoring and collection of information and/or obtain personal or sensitive information shall come via an “IT Monitoring - Directed Investigation Request” from a Senior Officer of the University. An IT Monitoring – Directed Investigation Request form shall be used, which may be found at: www.ulster.ac.uk/isgsc/policies.php

A register of “IT Monitoring - Directed Investigation Requests” shall be maintained. Directed Investigation Requests shall be time and scope limited. Staff shall retain a secure and protected copy of this letter for their records. Requests by other means shall not be processed.

Reporting Procedures

Unacceptable use, illegal use or other University Policy non-compliance with respect to University IT policy shall be reported as soon as possible. The Procedure for reporting such issues detected during monitoring are contained in Appendix A - Reporting Unacceptable and Illegal Use, “Acceptable Use of Information Technology Code of Practice”.

Terminology

The term:

“JANET” is used to refer to the Joint Academic NETwork. JANET is the U.K. computer network dedicated to education and research. All further and higher education organizations in the UK are connected to JANET, as are all the Research Councils.

“NTP” is used to refer to The Network Time Protocol, and is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks like the Internet.

“IP Address” refers to an” Internet Protocol” address assigned to devices participating in a network as a unique identifier for the purposes of network communication.

“Data Subject” is used to refer to an individual who the personal data or information is about or, put another way, the subject of the data or information.

“DPA” refers to The Data Protection Act 1998 (DPA) which is a United Kingdom Act of Parliament which defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK.