IT MONITORING POLICY

1 Summary

University communication networks and IT systems are monitored, to ensure their smooth operation and security. Staff engaged in monitoring must be properly authorised.

2 Scope

All servers, workstations, mobile devices and other IT systems either owned by the University, connected to the University's networks or located on University premises. This includes University-owned machines used at home and personal systems that are connected to the University's networks (including wireless).

This policy also applies to any partner organisations connected to the University's networks, and such connections will monitored for compliance with the terms of their agreement and the JANET acceptable use policy.

3 Important Information for Users

3.1 General

Users are informed that their use of the University's data communications infrastructure, IT services, systems and applications may be monitored by authorised staff as permitted by UK legislation and in accordance with this policy. Further details of what is monitored is in Annex (A).

The University reserves the right to examine any file residing on any system within the scope of this policy. As a condition of connection to the University network, system owners must agree that IT Services, the Information Security Team or other authorised staff may inspect their systems on request and at any reasonable times.

The University also performs active scanning of its networks and connected systems – see Annex (A).

It is recognised that, in the course of their work, system administrators and other authorised IT staff will occasionally come across content of files, emails or other communications. Appropriate steps are taken to minimise the likelihood and impact of this.

3.2 Purpose

Monitoring takes place for the following purposes:

- Ensuring the smooth operation of, and safeguarding the security, integrity and availability of the University's data communications network, computer systems and other IT infrastructure
- Fault investigations

- Security incident handling
- Capacity planning for network expansion and service upgrades
- Detecting and investigating unauthorised use
- Compliance checks against University policies and regulatory requirements
- Law enforcement requests

3.3 Log Retention

In accordance with Data Protection legislation, log files with information relating to living individuals are normally kept for up to three months. In some situations where a business need exists, logs may be retained for longer; in such cases it will be up to the system owner to justify and document this.

Anonymised information, including that relating to statistics and trends is retained for longer periods.

4 Authorised Staff

The Chief Operating Officer and University Secretary has granted the Director of IT Services the following delegated authority:

To authorise members of their staff to perform Network, Systems, Applications and Data Communications monitoring procedures that conform to this Policy and all relevant UK laws and regulations.

Directors of other areas may obtain delegated authority to authorise appropriate staff to monitor only those service elements for which complete responsibility lies within their area.

It will be considered a disciplinary offence for anyone to engage in monitoring activities without proper authorisation, or to monitor outwith their areas of responsibility. Furthermore, it is likely that any individual who violates this policy will be breaking the law.

5 Ethics and Safeguards

Authorised staff including network and system administrators must execute their duties in accordance with the University's *Guidelines for System and Network Administrators*. In particular, authorised staff must:

- Respect the privacy of others, at all times
- 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 against any potential unauthorised access
- Destroy information collected in the monitoring process in accordance with the relevant retention schedule.

Annex A - What is Monitored

IT Services and Applications

All systems providing network services or applications may be monitored for:

- CPU utilisation Active processes
- Filestore - utilisation, anomalies, file types and file sizes
- Licensed software compliance
- Network statistics e.g. peak and average bandwidth utilisation and errors
- System and security log anomalies
- Successful and unsuccessful access attempts - user account, remote IP address, date/time stamp, session duration
- Unusual network traffic

Details of logs kept by certain specific central IT systems are below. Note – this is not an exhaustive list.

Email

The University email systems keep logs of message delivery including:
Timestamp, sender+recipient email address & mail server IP address, message size, message-id

Web Access

Web access is logged, including access to and from external sites, for the following purposes:

- Investigating cases of suspected unauthorised use or illegal activity that are reported
- Investigating cyber security incidents
- Compromised host identification

The information logged includes:
Timestamp, client+server IP address, URL, User-Agent, Referrer

Intrusion Detection Systems

The University operates Intrusion Detection Systems (IDS) that look for recognisable signatures of attack profiles. This is to identify malicious activity, including cyber attacks and compromised hosts. When a signature is recognised an event is logged including:
Timestamp, source/destination IP address/port, signature-id, suspect payload

Network Monitoring

University networks are monitored for protocols and applications in use, sources and destinations (traffic patterns), performance metrics, volume sent/received per router and switch interface, and failure conditions.

Also, logs of network traffic are kept on a “per-flow” basis, including:

Timestamp, Source + destination IP addresses, TCP/UDP port numbers, volume

Under exceptional circumstances e.g. to help investigate incidents or fault conditions, the full content of specific interactions between endpoints may be recorded for analysis. Records are retained for as long as the issue is active, after which time the information is destroyed.

Data communications infrastructure records and associations

Detailed records and inventories are maintained for all components of the data communications infrastructure including fibre optic cabling systems, building premises distribution schemes, backbone and edge routers and switches.

Associations are recorded between specific network connection points, MAC addresses, IP addresses and DNS names, and changes are tracked.

Active scanning

Authorised staff may perform active scanning of network segments to identify vulnerabilities or non-compliance with other University policies. Authorised staff must exercise due diligence, in particular:

- Inform the network and systems administrators responsible for the systems on a segment of the planned scan activity and provide the following:
  - Schedules including Time and duration of scans
  - Systems performing the scan, (IP addresses)
  - Object of the scan i.e., vulnerabilities to be tested
- Take reasonable steps to ensure the continued operation or functionality of systems being scanned
- Identify systems with vulnerabilities to the relevant system administrators

Users of personal systems should note that active scanning would apply to any personal system connected to the University’s networks. Any user who considers this condition unacceptable should not connect their system to the network.

Further information

For further information, please contact the Information Security Team.

Title:	IT Monitoring Policy
Version:	1.45
Status:	Approved by IDGG
Last update:	2018-09-18
Last review:	-
Author:	Chris Edwards