University of Kent
Information Services

Security Procedures for Systems Administrators

1. Introduction

This document defines the processes that may be undertaken in terms of monitoring the usage of IT systems owned or operated by the University. This includes systems operated by Information Services, other Professional Services and Academic Schools. It defines who is authorised to initiate these processes and the records that must be kept. This document also clarifies those monitoring processes that are undertaken as a normal part of operating the various IT systems and the uses to which any data obtained may be put.

2. Definitions of roles

See The University of Kent Information Technology Security Policy.

3. Collection and use of information

3.1. Data is collected on a routine basis for purposes connected with the provision, operation and security of IT services.

3.1.1. This data enables Systems Administrators to ensure that services operate securely and effectively and assists in the planning of future services.

3.1.2. Data may be used for accounting for the use of charged facilities.

3.1.3. Data may be used for statistical analysis. Such analysis will render the data anonymous after which the results may be published.

3.1.4. The data collected may be examined on suspicion of a breach of University regulations. The Investigating Officer will authorise such investigation.

3.2. Data may be collected in the interests of national security or to prevent or detect crime.

3.3. Where a law enforcement agency issues an interception warrant to the Network Controller all reasonable assistance will be provided to give effect to the warrant.

3.4. Data may be collected with the consent of the parties involved for the purpose of investigating problems reported by users of IT facilities.

4. Investigation of suspected misuse

4.1. The Investigating Officer may receive a complaint arising from:

4.1.1. Evidence from the behaviour or performance of systems;

4.1.2. A complaint by a member or former member of the University;

4.1.3. A complaint by a member of the public;

4.1.4. An interception warrant served on the Network Controller.

4.2. A secure record of all investigations is kept.

4.3. The Investigating Officer acknowledges the complaint where applicable and initiates appropriate investigations.

4.4. The Investigating Officer has discretion to suspend a user's access to an IT facility or facilities during an investigation.

4.5. The Investigating Officer has discretion to require the disconnection of IT equipment from the University data network during an investigation.

5. Withdrawal of facilities

5.1. Facilities include (but are not limited to) a user's IT Kent account, network connections, published materials and filestore.

5.2. Normally facilities will only be withdrawn on the order of the Investigating Officer.

5.3. In exceptional circumstances Systems Administrators may temporarily withdraw facilities if:

5.3.1. This is necessary to ensure the security or continued operation of the system or other systems in the University;

5.3.2. Undesirable material has been published including but not limited to material that might be considered: defamatory; that breaches copyright; that could be considered to constitute sexual or racial harassment; that discriminates on the grounds of race, gender, disability, sexual orientation, age, marital status, political or religious belief or contravenes the University's Equality and Diversity Policy; that could damage a computer/device (e.g. malware[1]); that constitutes advertising; that promotes an illegal act; that may violate any applicable laws; breaches University Regulations; or could bring the University into disrepute;

[1] Software designed to infiltrate a computer system without the owner's informed consent

5.3.3. This is necessary to safeguard evidence of a possible breach of University regulations or the law.

5.4. Where such action is taken the Investigating Officer will be notified as soon as possible (normally within one working day).

6. Collecting evidence of suspected misuse

6.1. All Systems Administrators involved in the collection of data relating to possible misuse of IT facilities will keep a permanent record of:

6.1.1. The dates and times of all events;

6.1.2. Who authorised the investigation;

6.1.3. What was authorised;

6.1.4. The steps taken;

6.1.5. The outcomes.

6.2. Evidence should where possible be left in situ during an investigation; however:

6.2.1. If the matter is likely to become a police investigation, the police should be involved at an early stage to ensure that evidence is collected, stored and used in an appropriate way.

6.2.2. If the presence of the data is an ongoing security threat, breaches publication guidelines or prevents normal operation of IT systems it may be removed to an alternative location while investigations continue.

6.2.3. Access to modify the original data may need to be restricted to ensure the integrity of the evidence at a later date.

6.2.4. The removal of access to suspect material may require the suspension of a user’s IT Kent account or the disconnection of a computerised system or device from the network (or the possible temporary confiscation of IT equipment).

7. Escalation

7.1. The standard University disciplinary procedures may be used for:

7.1.1. Cases of serious or repeated misuse of IT facilities;

7.1.2. Appeals against actions taken under these procedures

8. Retention of Data

8.1. All data collected will be destroyed once the objectives in collecting that data have been achieved.

8.2. Statistical results obtained from the analysis of data may be published or retained in an archive to facilitate long term planning.

8.3. Evidence of misuse of IT facilities will be passed to the Investigating Officer.