Access to Electronic Information Standard Operating Procedure

Information Services

This standard operating procedure (SOP) ensures that that third party access (i.e. that from a party that is not the individual owner) to electronic information processed, transmitted or stored under a user's account is only permitted through this formal route.

1. Purpose

This SOP ensures that all accesses will be authorised by an appropriate authority and be subject to due diligence and examination before being provided. These steps will ensure that the University complies with legal, ethical, human resources and regulatory responsibilities regarding:

a) complying with UK data legislation and Human Rights Legislation;
b) the appropriateness of investigations into the misuse of the facilities or breaches of the University's regulations;
c) maintaining the business function of the facilities.

The University's Information Services Professional Services Unit (IS PSU) has devolved responsibility for managing access to information and information systems. This responsibility allows dedicated individuals to access electronic information on the network under certain approved conditions, and as part of their operational activities.

2. Scope

All electronic information that traverses the University network may be intercepted and monitored in compliance with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

3. Definitions

3.1 Requestor. The individual making the request for access should be responsible for the user whose account is being accessed. For a member of staff, this will be the line manager (or, in his or her absence, a more senior manager or a nominated deputy of equivalent or higher standing). For a student, this will be the Course Director or research student supervisor or equivalent role (or, in his or her absence, the Directors of Education or Research of the relevant School). If the person seeking access is none of the above then they should be directed to the appropriate requester, as outlined above.

3.2 Authoriser. The person who can authorise access. The authoriser shall be the line manager of the formal requester (see definitions above) or, in his or her absence, the Pro-Vice Chancellor of the School or Service Director of the Professional Service Unit. The Vice-Chancellor, Chief Operating Officer or University Secretary may personally authorise any legitimate request.

Where a covert investigation is required, then this must only be authorised by the Vice-Chancellor, Pro-Vice Chancellor of the School, Service Director of the Professional Service Unit[1], the Chief Operating Officer(s) or the University Secretary.

4. Responsibilities

The authoriser of any request must consider the following:

a) Cases where permission has not been sought

- Is it appropriate to contact the individual to seek access permission, or have reasonable attempts been made to contact the individual without success?
- Is the request justifiable and proportionate?
- Does the issue need immediate attention?
- Is there a sound reason for the access? Generally, the following would constitute acceptable reasons for access: compelling business imperative, compliance with applicable legislation, disciplinary investigation, to support or defend against internal or external complaints about the affairs or conduct of the University and/or any of its staff or students.
- Does the case provide sufficient documented evidence to support the request being made?

b) *Cases where permission has been sought, but refused by the user*
In addition to the issues outlined above:

- Does the refusal of the user represent a legitimate right to privacy?
- Is there evidence that the reason for the access outweighs the individual's right to retain that information and privacy?
- Is there a legal imperative to proceed with permitting access in spite of a clear indication from the user that they are not happy with this?

Requests should be rejected if:

- they may constitute an unreasonable invasion of privacy
- the request cannot be justified and evidenced
- the issue can reasonably be delayed until the employee/student provides access or there are alternative solutions available.

The requestor (i.e. person who is accessing the information) must consider the following once access has been provided:

1. Always use discretion and careful judgement before reading the content of any particular item (e.g. by using the subject header or filename) to avoid accessing content that is clearly not relevant to the reason for being granted access or is marked of a private/personal nature.

The originator of the request (usually the line manager, Course Director or supervisor) remains responsible for ensuring that any further staff, of an equivalent grade, given access are made fully aware and comply with the conditions above and ensure that confidentiality is always maintained.

On a general note, requests for access will be time dependent and not open-ended, and as such a specific timeframe (e.g. 28 days) must be included as part of the original request. Where an extension to this timeframe is required then further authorisation will be required.

[1] For Human Resources, due to the immediacy and sensitivity of the information, a nominated deputy (Head of HR Operations) has been given the authority to make such decisions in the absence of the Director of HR & OD

Document control

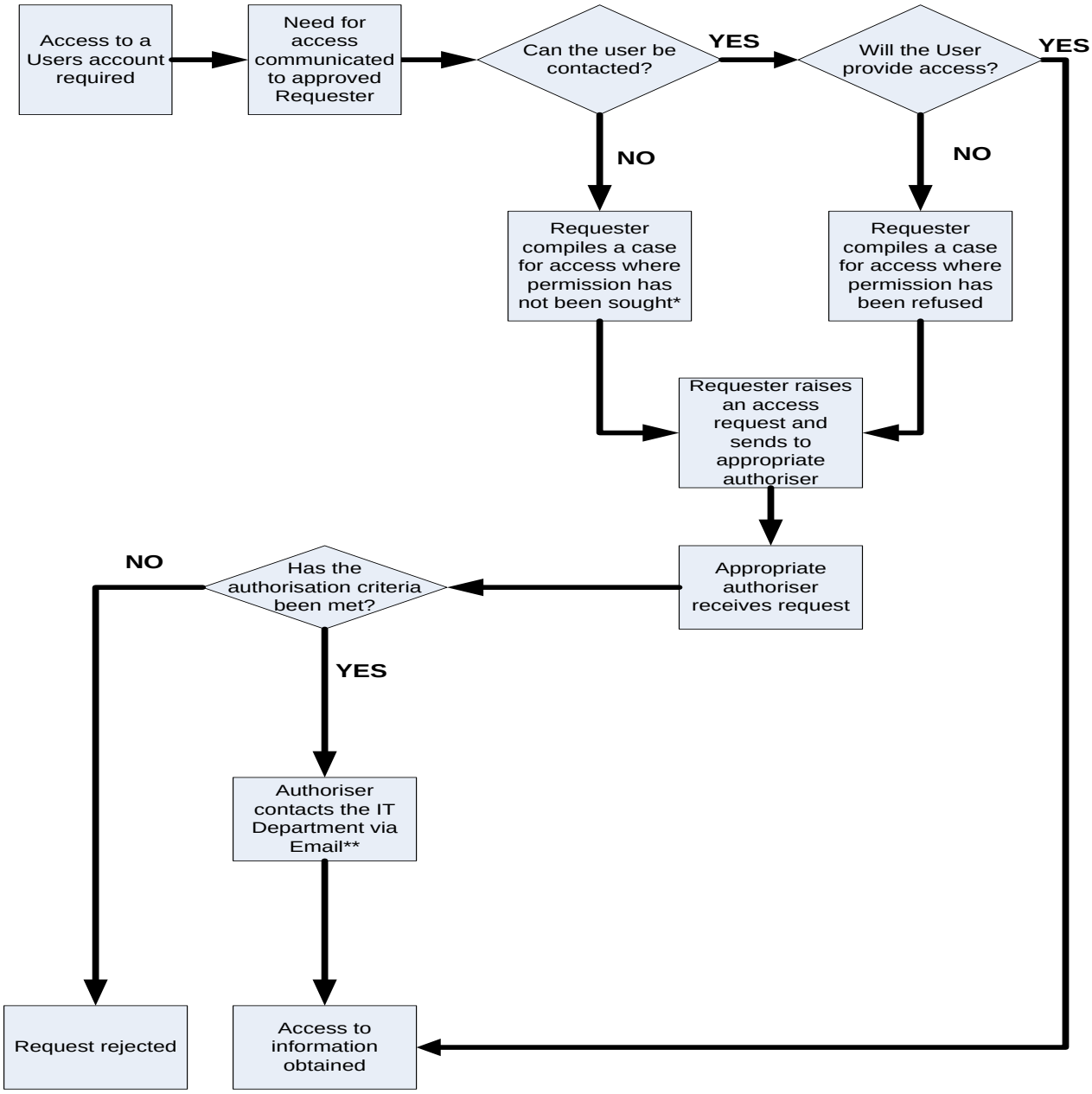
Document title	Access to Electronic Information Standard Operating Procedure
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Approval by and date	Director of Information Services; 01/10/2019
Date of last review and version number	September 2019: 1.4
Date of next review	August 2020
Information categorisation	Confidential - Commercial

Document Review

Version	Amendment	By	Date
1.3	Minor amendments to content	Information Security	November 2018
1.4	Format/date changes only	Information Security	September 2019

Appendix A

1. Specific procedure



* In exceptional scenarios it may be deemed not appropriate to contact the user i.e. where an investigation is required and this may prejudice the investigation itself.

** For normal requests this will be via the IT Service Desk (E. servicedesk@cranfield.ac.uk; T. 01234 754199), but if the request is of a sensitive nature then the Authoriser should send the request direct to the Director of Information Services or the Information Security Team (E. itsecurity@cranfield.ac.uk).