Integrated
Research Campus

UNIVERSITY OF LEEDS

Information Security Communication Procedure

Version 1.0

Version Date 20/10/2016

Document Information

Reference	IRC ISC PROC
Category	ISMS Documents
Title	Information Security Communications Procedure
Purpose	Procedure for information security communications in the IRC
Version	1.0
Status	Approved, External
Owner	IRC Information Governance Management Group
Author	Samantha Crossfield
Compliance	ISO 27001 for scope defined in IRC Framework of the Information Security Management System
Review plan	Set in the IRC IS Documentation Procedure
Related Documents	University of Leeds Information Protection Policy IRC Framework of the Information Security Management System

Version History

Version	Date	Change description
0.1	27/06/2016	Initial version
1.0	20/10/2016	Submitted for sign off

Sign-Off

Name	Date	Role
Barry Haynes		Chair of IGMG and Head of Enterprise Architecture, University of Leeds

Master version:

Signature…….

Table of Contents

1. Purpose

The Integrated Research Campus (IRC) is a University of Leeds Central IT provision. It provides secure technical infrastructure and services for research data handling, analytics, application processing and development. This document is part of the IRC information security management system (ISMS).

The IRC Framework of the Information Security Management System sets the IRC IS objectives and which of these are met through the procedures defined in this document.

This document sets the procedure for formal communications regarding information security that relates to elements within the scope of the IRC ISMS. The purpose is to ensure that relevant issues of information security are communicated to relevant individuals with clarity and consistency. This ensures that people have the necessary knowledge to carry out their responsibilities for information security.

2. Application

This document applies to those formally required to communicate information security regarding elements (including infrastructure, assets and people) that are within the IRC ISMS scope. Section 5 sets the responsibilities for effective IS communication.

3. Recipients and Triggers

Information security management communications are provided to those defined as ‘relevant individuals. That is, individuals directly affected by the matter being communicated or with responsibilities for any affected procedures.

IS management communications are carried out as follows:

1. Every reasonable attempt is made to communicate planned new or amended security procedures with relevant individuals prior to implementation
2. Emergency system changes are communicated with relevant individuals as soon as possible
3. Existing procedures are communicated when an individual first enters their scope of applicability

4. Scope

IS management communications should cover the following (where it is known and relevant) in a manner that is clear and comprehensive:

1. The purpose or objective of the procedure
2. Description of the procedure as it relates to the recipient
3. Responsibilities for implementing and managing the procedure
4. Feasible timeframe for implementation
5. Review plan for the procedure
6. Opportunity for queries and comments
7. How to confirm agreement of the procedure

However, information must not be disseminated where doing so may facilitate a compromise to information security (unless appropriate controls or sanctions are in place).

5. Responsibilities

This section assigns the responsibilities for effective communication about IS:

The role of the IRC Information Governance (IG) Management Group is:

1. To communicate the importance of effective IS management and of conforming to IRC ISMS requirements (or the consequences of not doing so)
2. To maintain this procedure for making information available to relevant people in a timely manner and via appropriate channel
3. To ensure the IRC Data Services Team have the relevant information
4. To maintain open channels of two-way communication and to listen to feedback and comment from staff and users

The role of the IRC Data Services Manager is:

1. To communicate regularly with their team, preferably face to face, to ensure information relating to the ISMS is available and understood
2. To ensure they and their team are maintaining good communication practice regarding information security, in accordance with this document
3. To listen to feedback from their team and users and to keep the IG Management Group informed, as per the line of reporting set in the IRC Audit and Management Procedure
4. To ensure all the electronic forms of communication channels are up to date and capable of delivering information in time

5. To communicate the outcomes of any IRC Risk Assessment or Risk Treatment Plan, as set in the IRC Audit and Management Procedure

The role of the IRC Data Services Team is:

1. To ensure they are informed and have access to information in order to be as effective as possible in their role
2. To ensure they are maintaining good communication practice as set out in this document
3. To keep line managers, colleagues and users aware of up to date information
4. To maintain an electronic copy of the ISMS documentation, accessible to those (internal and external) to whom the scope of the ISMS applies

The Role of IRC users is:

1. To keep the IRC Data Services Team informed about their needs for data handling
2. To address any IS requirements raised with them by the Data Services Team and to communicate the outcome (for example, completing any IS training)

6. Channels

Channels include: directive conversation or presentation, documentation (including information leaflets), email, site notification for general broadcasting (for example, via a user portal such as on the IRC intranet, website or notice board), training course, poster, webinar, coaching. The following subsections provide **steps to be followed when utilising specific channels**:

6.1. Email

Email is a commonly used channel, with the following steps being used by IRC staff:

- Email are regularly checked to ensure issues are picked up
- Phone or face-to-face options are preferred for urgent IS issues
- Reduce acknowledgement emails or cc'ing people unless specified
- Ensure that distribution lists are targeted and updated
- Set clear subject lines with key words that aid identification of the topic
- Consider alternatives to attachments, such as a link or copying relevant text
- Use bullet points or numbers rather than narrative to set out points or actions
- Keep to one subject per email
- Only data defined as **IRC Unclassified** can be sent unencrypted by email

6.2. Documentation

The IRC IS Documentation Procedure sets out the procedure for creating or amending documents that are part of the ISMS. It is useful guidance for wider documentation also. Procedures relating to the ISMS must be documented. The IRC Access and Usage Policy defines when a Working Instruction should be created.

6.3. Presentation

Presentations (including webinars and symposia) offer opportunity for interaction and disseminating information on IS management to a wider, defined audience. A presentation must introduce the topic, specify any required learning or action for the audience to undertake, and should signpost toward any relevant documentation for further information. The audience should be given a channel for feeding back comments or queries.

6.4. Telephone or Face-to-Face

Introductions must cover name and organisation, department or team details where these are not known to all present. Be aware of possible disclosure through being over-heard and use a private office or meeting room for disclosive discussions.

7. Channel Selection

The channel to be selected for communication is that which will most speedily and comprehensibly convey the relevant information. This is influenced by the information content, the audience, and the responsibilities placed on the recipient.

7.1. Content

The message content must highlight any actions that are required from the recipient, and indicative timescales for completion.

The content will influence the channel to be chosen. Consider the following:

1. Urgency – for immediate or imminent procedure changes, email and site notifications may suffice.
    - **Urgent security issues** must be raised with the IRC Data Security Team through face-to-face or telephone channels.

2. Complex or novel information – directive conversation, training and webinars can provide opportunity for in-depth learning and questioning. By comparison, posters, newsletters and site notification can be used to issue reminders.
3. Generalisability – communications for a wide audience may be efficiently disseminated through email, presentations, e-training or videos.
4. Frequency – site notification can point towards document updates for evolving procedures.

7.2. Audience

For communications **among IRC staff**:

- IS management communications are conducted primarily by face-to-face or telephone methods
- Email or training resources may be used for non-urgent issues, especially if affecting many staff

The audience will influence the channel to be chosen. Consider the following:

1. Location – avoid unnecessary travel by utilising electronic communication such as webinars or videos, portal notifications and emails
    - At a shared locale, face-to-face meetings are preferred
2. Role – a person's role and relevant expertise may influence whether a channel more conducive to interaction and feedback is appropriate
3. Impact – directive conversation, training or detailed documentation may be more suitable than posters and site notifications for people whose daily working is highly affected by the procedure

7.3. Actions

Where actions are triggered as a result of IS management communication, these should be followed up with a formal written notice of agreed action, and completion in due course. Where actions arise from communication between IRC staff, no formal notice is required (separate to any procedural logs) though a face-to-face, telephone or emailed notice of completion should be considered.