Integrated
Research Campus

UNIVERSITY OF LEEDS

Event Handling Procedure

Version 1.0

Version Date 20/10/2016

Document Information

Reference	IRC REH SOP
Category	ISMS Documents
Title	Risk and Event Handling Procedure
Purpose	IRC procedure for handling highlighted security risk and events
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 Documentation Procedure
Related Documents	University of Leeds Information Security 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 data handling. This document is part of the IRC information security management system (ISMS). The IRC Framework of the Information Security Management System sets the IRC information security objectives and which of these are met through the procedures defined in this document.

This document sets the **procedures for handling security events** that threaten or breach information security in the context of the IRC ISMS scope. **They are to be followed if unexpected risks are raised or incidents occur**. This includes procedures for reporting, communication and escalation.

2. Applicability

This document and the procedure for reporting events and risk applies to all IRC users, staff and contracted third parties. It also sets the procedure for investigation and event response, which applies to the IRC Data Services Team. The IRC Information Governance Management Group maintain this procedure and oversee its implementation.

3. Risk Handling

While a risk is not an event, reference is made here to risk handling. This is in recognition of unanticipated risks that are spotted outside of risk assessment and in this way are similar to events.

During day-to-day work, IRC users, staff and contracted third parties must remain vigilant to information security risk, as set in IRC user agreements and service level agreements. Everyone responsible for raising security concerns with the IRC Data Services Team, as set their IRC user agreement and the IRC Framework of the Information Security Management System.

When a risk is reported, the IRC Data Services Team assess and handle the risk in accordance with the IRC Risk Assessment Procedure and IRC Risk Treatment Procedure. The team publish a prioritised treatment plan for any required actions.

4. Breach and Event Recognition

During day-to-day work, IRC users, staff and contracted third parties must remain vigilant to information security breaches. This is set in IRC user agreements and service level agreements. Breaches may also be identified through risk assessment or automated or manual monitoring and audit at the organisational- or project- level.

If a breach affects information security then it is an event and it triggers event handling (Section 5). **An event is a breach, or utilisation of a loophole, in the ISMS or the ethico-legal framework surrounding an information asset, regardless of intent**.

5. Event Handling

All users and staff are responsible for reporting events to the IRC Data Services Team. This is set in their IRC user agreement and the IRC Framework of the Information Security Management System.

The IRC Data Services Team manager reports all events to the IRC IG Management Group who determine whether there is an ethico-legal or reputational issue. This decision is minuted and reported to the University of Leeds ITS Group and Information Protection Group. The decision is informed by the risk criteria in the IRC Risk Assessment Procedure and the ethico-legal framework around any involved information assets. If there is, then an **incident** is deemed to have occurred.

Two simultaneous actions are taken in response to an incident:

1. The IRC Data Services Team write an **IRC Incident Response Plan** (Appendix 1). This produces a prioritised treatment plan of required actions
    - This is reviewed and authorised by the IRC IG Management Group
    - The IRC Data Services Team instigate and assign the actions and oversee their completion
2. The IRC Data Services Team trigger the controls set in the University of Leeds Security Incident and Misuse Policy
    - This informs the University of Leeds IT Security Team
    - This informs the University Data Protection Officer (DPO) of any breach involving personal data

Regular updates from both actions are reviewed by the IRC IG Management Group. During and following an incident the Group consider the following:

1. What happened
2. Lessons learned
3. Any further action to be taken (including any change to ISMS documentation).

If an event is due to changes in ethico-legal requirements then the incident response plan may trigger:

1. Changes to the IRC ISMS as per the IRC IS Audit and Management Procedure

2. Changes to a project protocol, conducted by the research team (or appropriate other) and overseen by the IRC Data Services Team

5.1. Interim Measures

The IRC Data Services Team may implement interim measures at any point to protect people, infrastructure or information while event handling is underway. These are temporary measures that contain or reduce a real or potential event or risk through means that have either not yet been reviewed by the IG Management Group or are not efficient or acceptable as a long-term solution. For example, they may hinder data access or be costly to maintain.

Interim measures are planned and implemented **as soon** as it becomes apparent that:

1. IRC Secure or IRC Confidential data is involved in an event that is anticipated to be deemed to be an incident (following IRC IG Management Group review)
2. An incident is occurring (Section 5) and the approved actions for incident resolution have not yet been agreed, undertaken or otherwise completed

The IRC IG Management Group must be informed of interim measures as soon as possible (and within 24 hours). These feed into event handling (Section 5) and the IRC Incident Response Plan. This is in accordance with the process for procedural deviations that is set in the IRC IS Audit and Management Procedure**.**

Interim measures stop once the approved actions for incident resolution have been completed.

5.1.1. Communications

Users that are affected by interim measures are informed of progress and any changes in the anticipated duration of the measure. The regularity of progress updates depends on the level of service reduction.

6. Event Logging

The IRC Data Services Team log all reports and handling of events in the **IRC RAID Log**. The log maintains a record of any open and closed risks, events, issues and actions, as well as risk ownership, decisions and assumptions. Items are maintained in the log indefinitely.

The University of Leeds IT Security Team also maintain a University log of the number and type of any breach raised via the University of Leeds Security Incident and Misuse Policy. Similarly, the University Data Protection Officer (DPO) maintains a log of any breach involving personal data in the University.

7. Reporting and Escalation

Event handling is reported internally, and can be escalated, to the IRC Information Governance Management Group. The Group review the **IRC RAID Log**, sign off **IRC Event Response Plans** and own residual risk based on the likelihood and impact of future events. The Group report, and can escalate, to the University of Leeds Information Protection Group and IT Security Group.

7.1. Third Party Reporting

If an incident involves an information asset then the IRC Data Services Team inform the data controller/s and user/s of the data. They are requested to inform any necessary governance body, Sponsor, Funder or such third party – as set in the terms for handling that data – and provide the Team with evidence of this. The nature and timescale for reporting will depend on the ethico-legal requirements which may be set, for example, in a data sharing agreement. The Team will provide any necessary and reasonable support and information regarding the incident. The Team will not provide details where doing so would breach ethico-legal requirements or threaten the ISMS.

Appendix 1: IRC Event Response Plan

IRC Event Response Plan

Event Response Plan Details

Title	IRC_EventResponsePlan_[ccyymmdd of approval]
Assessor	IRC Data Services Team
Approval	IRC Information Governance Group Chair
Date of approval	
Related documents	IRC Framework of the Information Security Management System, IRC IS Risk Assessment Procedure, IRC IS Risk Treatment Procedure

1. Event Description

What happened and how did it happen? How was it spotted?

2. Prioritise Options

Assess treatment recommendations. The IRC breach acceptance level is low so fill in the table for all breaches:

Priority: *Rating of breach impact on confidentiality, integrity and availability, 1 (low) to 5 (high)*
Option: *Outline the option*
Sort the table based on priority and assign an ID, 1 to n

Breach ID	Option ID	Priority	Option

3. Option Evaluation

Costs: *outline the resources required, including staff time, training, maintenance, infrastructure, licence or hardware purchases, reduction in operational effectiveness,*
Compatibility: *outline the compatibility with IRC aims and user acceptance*
Effectiveness: *outline the afforded degree of protection and breach resolution*
Benefit: *score 1 (low) to 5 (high) based on the above, particularly the effectiveness*

Option ID	Costs	Compatibility	Effectiveness	Benefit

4. Cost-Benefit Analysis

Multiply the priority score (breach impact) by the benefit score (based on cost, compatibility and effectiveness for each and order by impact

Option ID	Breach ID	Priority *1-5*	Benefit *1-5*	Impact *P x B*

5. Select and Assign Actions

1. Select the most effective action/s to address the breach, by recording the Option ID for each breach that has the greatest impact. Select multiple options per breach ID where these are complementary.
2. Record the selected option IDs by order of impact, high to low
3. For each action, determine:
    a. Implementation start and completion date
    b. New maintenance or monitoring requirements to ensure effectiveness
    c. Where responsibility lies (person, team or organisation)

Action	Option ID	Start date	End date	Maintenance / monitoring	Responsible persons
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

6. Statement of Applicability

The IRC Information Governance (IG) Management Group sign-off the breach actions, based on the justifications in this treatment plan

IG Management Group Chair:

Name……………………………………………………………….

Signature…………………………………………………………...

Date…………………………………………………………………