Incident Response Plan

Process to Manage Information Security Incidents / Data Protection Breaches (Actual or Suspected)/CPRE System Security Breaches)

1. Introduction

An Information Security incident is any event that adversely affects the Availability, Integrity and / or Confidentiality of Systems and Data. This includes:

- loss of availability of systems and / or data;
- loss of confidentiality of information, such as supporters details or credit card information;
- compromise of integrity of information;
- denial of service;
- unauthorised access to systems;
- misuse of systems or data;
- theft and/or damage to systems; or
- virus or other malware attacks.

Other incidents include:

- Missing correspondence;
- Misplaced or missing media;
- Inadvertently sharing passwords;
- Loss of mobile phones and portable devices; or
- Alert from security monitoring system including but not limited to intrusion-detection and firewall breach.

Note: These lists are examples **ONLY** and not exhaustive as Incidents can be highly complex.

1.1 Definitions

Data: Information which is stored electronically, on a computer, or in certain paper-based filing systems. For the purposes of this policy, **'Data'** will be used to describe Personal Data and Sensitive Personal Data together.

Data Users / Users: Includes employees, contractors, consultants, temporary or other workers and volunteers whose work involves using Personal Data.

Incident: an Information Security incident is any event that adversely affects the Availability, Integrity and / or Systems and Data, and includes but is not limited to the examples listed under paragraph 1 above.

Incident Response Team (IRT): the IRT is listed and detailed in Section 5 below.

Personal Data: Information about living persons that enables them to be identified e.g. name and address. It does not apply to information about organisations, companies or agencies, but applies to named persons such as Data Subjects.

Sensitive Personal Data: Includes information about:

a. the racial or ethnic origin of the Data Subject;
b. his political opinions;
c. his religious beliefs or other beliefs of a similar nature;
d. whether he is a member of a trade union;
e. his physical or mental health or condition;
f. his sexual life;
g. the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

CPRE Systems: include all systems owned or provisioned to conduct CPRE business and operations, including but not limited to any system you use as part of your work, computers, data processing, e-mail, mobile devices, messaging services, remote access capabilities, telephone, and voice-mail.

2. Compliance with Legal and Contractual Obligations

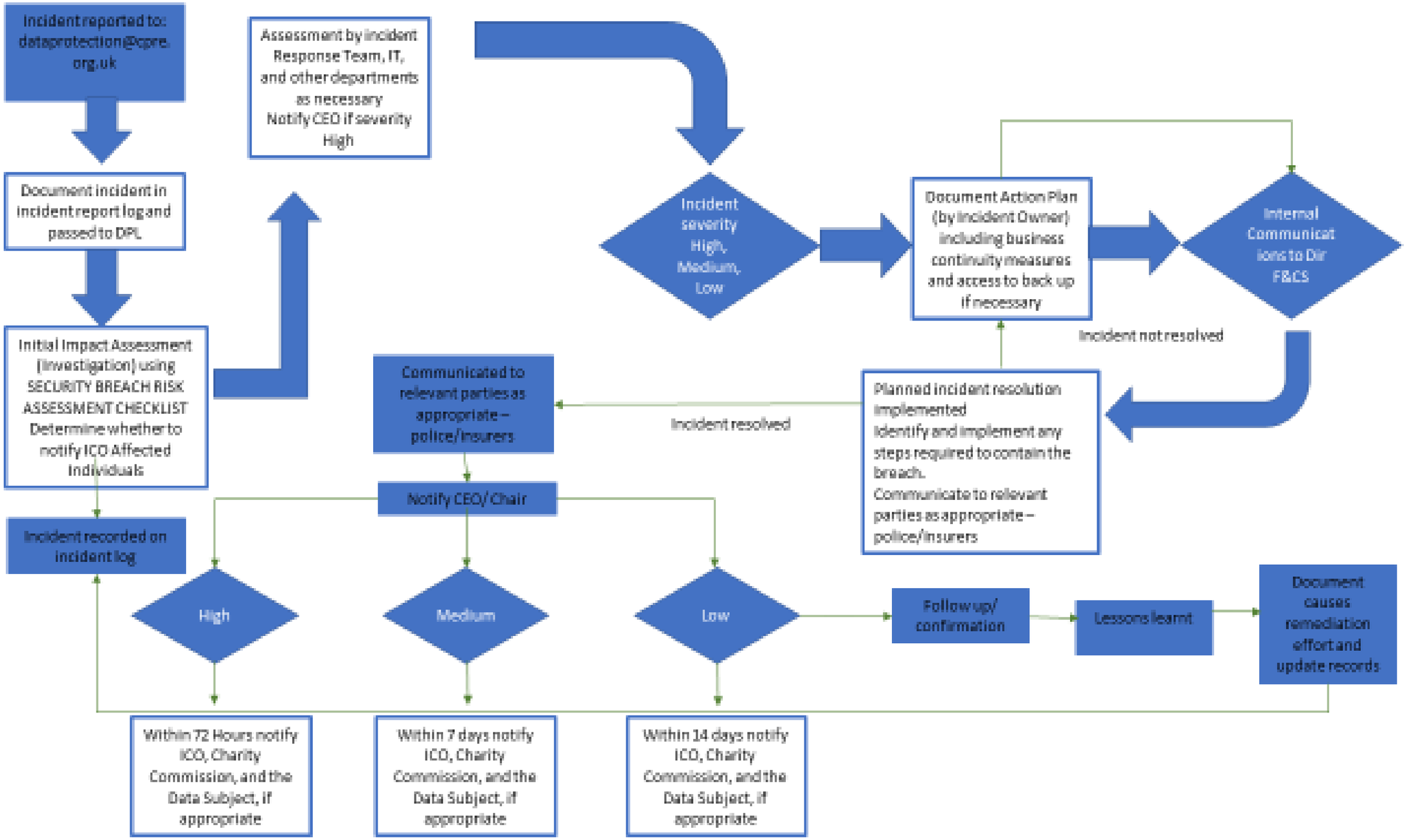
- The Data Protection Act (1998) requires that personal data be kept secure against unauthorised access or disclosure;
- The Computer Misuse Act (1990) covers unauthorised access to computer systems;
- General Data Protection Regulations

3. Process Flow

The critical steps required to manage an Information Security incident are:

- Detection;
- Assessment;
- Communication;
- Escalation;
- Resolution;
- Follow-up; and
- Review of lessons learned,

as illustrated in the diagram overleaf:



- Dotted lines in the diagram indicate where a step is not mandatory, however may need to be assessed whilst the incident is ongoing.

3.1. Reporting

Throughout the breach management process records should be kept of what action has been taken and by whom.

- Suspected data breach incidents should be reported to the IRT – markc@cpre.org.uk dataprotection@cpre.org.uk
- Low severity incidents may be handled by Finance & Corporate services team without wider Incident Response Team (IRT) input, although the incident will be recorded. If there is uncertainty about the severity assign it as medium and the IRT will consult with the Director of Finance & Corporate Services (DFCS)
- If severity is Judged to be high an assessment must be made by the DFCS as to whether it is necessary to notify the affected data subjects, ICO & Charity Commission. The CEO must be notified immediately if the severity is deemed high.
- Further assessment may include input from one or more of the contacts listed in section 5, this will depend on the nature of the incident including complexity, severity and impact.
- If the incident cannot be contained and is of significant severity, further reporting may be needed to external parties; timescales are for guidance and may vary in a real world situation.
- If the incident is both contained and resolved, the escalation stage may be omitted (e.g. mis-collation of a covering letter with Countryside Voice. Data subjects were contacted and the supplier instructed).
- Recorded Incident details must be kept updated throughout the process and finally updated with any lessons learned and remediation actions.
- All incidents should be periodically reported to the SMT (e.g. at monthly scheduled meetings) and Audit & Corporate Service Committee.
- Where the Director of Finance & Corporate Services in unavailable the Director of Development & Marketing will deputise.

4. Incident Categories

Explanation of the causes and origins of incidents

Cause	Origin	Description
Accidental Accidental	Internal External	Where a person(s) causes an information security Incident or event unexpectedly, unintentionally, without a particular purpose or by chance.
Deliberate Deliberate	Internal External	Where a person(s) causes an information security Incident intentionally with an intended / desired result or a particular purpose.
Error Error	Internal External	A malfunction, user error, flaw, user mistake, failure, fault or bad code in an IT system or software program that prevents it from behaving as intended.
Unknown Unknown	Internal External	Incident cause is unable to be identified. Requires further investigation.

5. CPRE Incident Response Team (IRT) and Further Steps

In the event of an Incident the relevant / appropriate contacts should be notified and kept informed of the status of an Incident from the time it is recorded on the system through to resolution and lessons learned. Not all Incidents are the same and will vary in nature and severity, therefore not all contacts listed will necessarily become involved, for example a minor Incident (Low) will involve far fewer people than a major Incident, and in some instances a wider group of stakeholders will need to be involved.

As part of CPRE's response to emergencies designated senior managers are available on a 24/7 basis to respond to alerts.

If a data breach is detected outside of office hours you must direct your call to 07887 781592.

Initial Impact Assessment (investigation) will include contacting the relevant staff members to confirm breach has occurred, gathering all necessary information to determine the extent of the data breach and taking any necessary additional steps to stop further data exposure.

5.1. IRT Contacts

Name	Role	Dept.	Reports to
Mark Cornish	Director of Finance & Corporate Services	Finance & Corporate Services	CEO
Jenny Bulman	Corporate Services Manager	Finance & Corporate Services	Director of Finance & Corporate Services
Adrian Howe	Outsourced IT provider	Caranet	Director of Finance & Corporate Services
Anthony Nunes	Database Administrator	Supporter Services	Director of Development & Marketing
Elvira Meucci-Lyons	Director of Development & Marketing	Development & Marketing	CEO

Depending on the incident, the IRT will co-opt the relevant senior managers to join as appropriate.

Changes to this Policy

CPRE will update and renew this policy from time to time.

Data Users will be notified, where appropriate, when such changes are made, and it is the responsibility of all Users to ensure that they have read and understood the latest version of this policy.

If you have any questions or concerns then please refer to the Information Security and Data Protection team at data.protection@cpre.org.uk