Scottish Funding Council

Data Security Incident Procedure

Contents

Data Security Incident Procedure

Introduction

1. This document sets out the procedure for handling and reporting a data security incident at the Scottish Funding Council (SFC).

Scope

2. This procedure covers incidents relating to both personal data, and confidential business information.

3. A personal data breach is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed by SFC, including data processed on behalf of SFC by a third party.

4. For SFC's purposes a data security incident is any incident which is, or risks leading to:

   - A personal data breach, as defined above.
   - The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, confidential business information.
   - Any incident which risks either of the above occurring.

5. Data security incidents include but are not limited to:

   - The loss or theft of data, or equipment on which data is stored.
   - Inappropriate access controls allowing unauthorised use.
   - Human error leading to unauthorised disclosure, including verbal disclosure.
   - Hacking attacks.
   - Accidental deletion of information.

6. The data involved in an incident can be personal data or business information. Personal Data is covered by data protection legislation, and SFC may be obliged legally to inform the UK Information Commissioner of a data security incident involving personal data (see Appendix B for further information).

7. A data security incident could compromise the confidentiality, integrity or availability of SFC's information. If such an incident should occur then these procedures must be implemented without delay. The focus of any response should be to minimise the impact on SFC and any individuals whose data is involved in the incident.

8. SFC must record all incidents that pose a significant risk to the security of SFC's data. This includes incidents that do not result in information being lost or

accessed by unauthorised individuals. By recording these incidents, SFC is able to identify areas of risk and help prevent breaches in future.

Responsibilities

9. All members of staff are responsible for keeping SFC's data secure and should comply fully with this policy.

10. All members of staff must report information security incidents as soon as they become aware of the issue. Further information on what type of issue should be reported is described in Appendix C. If you are unsure if an incident should be reported or not, you should discuss this with the Information Management and Governance Officer (IMGO) immediately. If the IMGO is not available, the issue should be reported to Assistant Director - Strategy.

11. The IMGO is responsible for oversight of compliance with this policy and for ensuring that it is kept up to date with business needs and legislative requirements.

Procedure

12. As soon as a data security incident has been detected, or is suspected, the following steps should be taken without delay.

13. The incident must be reported to the Information Management and Governance Officer (IMGO) immediately. If the incident is believed to be 'high risk' it should also report to the Senior Information Risk Owner (SIRO). See Appendix C for information on how to identify the risk category of an incident.

14. All reported incidents will be assigned an Incident Manager. For low or moderate risk incidents, the IMGO will normally be the Incident Manager. For high risk incidents the SIRO will normally be Incident Manager, alternatively it must be a relevant Senior Officer of M1 grade or above. The IMGO shall be available for consultation and should be kept informed throughout any investigation.

15. The Incident Manager should investigate and record as much detail as possible about the incident, completing the form at Appendix A. The report should include recommendations on measures required to prevent the incident reoccurring. Such measures could include security measures, changes to processes, training, or raising awareness. Reports for incidents considered high risk should be provided to the CEO.

16. The priority during any incident is to limit the impact of an incident on the individuals' whose data is involved and SFC as an organisation. The Incident Manager should identify and implement any steps required to contain any

breach and to identify and implement any steps required to recover any losses and limit the damage of a breach.

17. The Incident Manager must determine the arrangements for reporting the incident to relevant authorities. High risk incidents involving personal data must be reported to the Information Commissioner's Office within **72 hours** of discovery of the incident. The incident manager must also consider if the individuals involved should be informed of the incident; however this does not need to take place within 72 hours. Appendix B contains information on the notification of breaches.

18. High risk incidents must be reported to the CEO and sponsor department in Scottish Government without delay.

19. The Incident Manager and Data Protection Officer should advice the Assistant Director -Communications or Head of External Relations on managing any communications about the incident (see Appendix B for further guidance).

20. The IMGO shall record the incident in SFC's Incident log.

Contacts

Information Management and Governance Officer (and Data Protection Officer)	Callum Morrison	Ext. 6566
Chief Operating Officer (and Senior Information Risk Owner)	Martin Fairbairn	Ext. 6524
Assistant Director - Communications	Stephen Crowe	Ext. 6612
Head of External Relations	Lynne Raeside	Ext. 6526
Assistant Director - Information Systems	Laurence McDonald	Ext. 6535

Document Control

Title	Data Security Incident Procedure
Prepared By	Information Management and Governance Officer
Approved Internally By	Chief Operating Officer
Date of Approval	20 March 2019
Review Frequency	Annually
Next Review Date	March 2020

Version control

Version	Date	Control Reason	Author
1.0	14/08/2018	New policy – replaces Data Breach Procedure to widen scope to include incidents which risk data breaches	C Morrison

Appendix A: Data Security data incident report form

Date incident occurred	
Date incident discovered	
Incident Manager	
Incident reference	*In the format YYYY/###*
Date report completed	
Incident risk level	

Part one: overview	
Give a summary of what happened.	
What data was involved in the incident?	
Was personal information involved in the incident?	
Was special category information involved in the incident?	
Was commercially sensitive information involved in the incident?	

Part two: incident management	
What level of risk is the incident? (see Appendix C)	
If the incident involves personal data, how many individuals does it relate to?	
If the incident involves personal data, what categories of personal data are involved?	
Where is the data now and have any unauthorised individuals had access to it? If yes, how many?	
Was the data protected from unauthorised access, e.g. encryption?	
Has there been a breach of data protection legislation? If yes which principle(s) have been contravened?	
What are the potential adverse consequences for SFC? How likely are they to occur?	

If the incident involves personal data, what are the potential consequences for those individuals?	
What could the data tell a third party about an individual? Does the information have commercial or strategic value?	
What processes or systems are affected and how?	
Has the security of any of SFC's systems been compromised?	
Has a similar incident happened before?	
What is being done to recover the data?	
How successful have recovery attempts been?	

Part three: reporting	
Who in SFC has been informed of the incident?	
If the incident involves personal data, do we need to inform the data subjects of the incident? If we do not decide to inform them, please record why.	
Do we need to advise our Sponsor Team at Scottish Government?	
Do we need to advise any third party organisations?	
Does this breach need to be reported to the Information Commissioners Office?	

Part four: recommendations and learning points

Appendix B: Notification of Incidents

General Considerations

Notifying an individual or organisation of a breach should have a clear purpose such as a legislative requirement, contractual obligation, to allow an individual to take steps to protect themselves, or to manage potential reputational damage. The following (non-exhaustive) list identifies key people and organisations that may need to be notified of the incident:

- Human Resources.
- Head of Information Systems.
- Police – in the case of criminal activity.
- Individuals whose data has been compromised – see the section on required reporting under GDPR.
- Information Commissioner's Office (ICO) – see the section on required reporting under GDPR.
- Universities or Colleges.
- SFC's legal services
- Banks – where steps may be required to protect accounts.
- Media.

The Data Protection Officer and Communications Team should advise on who should be notified of a data security incident.

Required Reporting under GDPR

Where there has been a breach of personal data, the General Data Protection Regulation (GDPR) requires SFC to notify the Information Commissioner's Office (ICO) and the individual whose data has been breached under certain circumstances.

Any personal data breach that could lead to physical or non-physical harm (for example the risk of discrimination, identity theft or fraud, financial loss and damage to reputation) must be reported to the ICO within 72 hours of becoming aware of the incident. If it is not possible to notify within 72 hours of becoming aware of the incident SFC must clearly record the reasons for failing to report within this time.

In some circumstances SFC may also be required to notify any individuals whose data has been breached about the incident if it is likely to limit their rights and freedoms.

For more specific guidance on what should be reported to the ICO refer to the EU Guidelines on Personal data breach notification under GDPR

What to say

The Communications Team will be responsible for handling external communications and IMGO will be able to advise staff on statutory notification to the regulator advising regarding a data breach.

Careful consideration should be given regarding any notification message. It is vital that we understand the details of the breach and are able to provide useful information. However, it is also vital that we respond in a timeous manner and in line with the legislative requirements discussed above.

You should consider including the following:

- Details of what happened and when the breach occurred.
- What data was involved?
- What steps have been taken to contain the breach and prevent reoccurrence?
- Advice on what steps to take, e.g. contact banks.
- How you will help and keep them informed.
- Provide a way to be contacted.

Appendix C: Risk Assessment of Incident

In order to handle an incident appropriately it is vital that we assess what risks it presents. SFC will assign any incident a risk rating as described below.

Low level incidents happen most frequently. These do not need to be reported unless similar incidents occur repeatedly. These incidents will have a negligible impact on SFC or the individuals involved but may highlight weaknesses in our practice. Anyone concerned about such an incident should speak to the IMGO.

Moderate level incidents require internal reporting to allow us to contain any breach and to take action to prevent issues happening again. These incidents may have some consequences for SFC's reputation or for individuals whose personal data is involved in the incident. Consequences for individuals could include causing inconvenience or annoyance but would not present any harm to their physical or non-physical safety. Such an incident may cause SFC limited embarrassment but not significant reputational damage or lasting impact when working with third parties.

High level incidents will require internal and external reporting. Any high level incident involving personal data will be required to be reported to the Information Commissioner's Office (ICO) within 72 hours of SFC becoming aware of the breach. These incidents will have significant consequences for SFC's reputation or the individual's whose data is involved in the breach. Where personal data is breached it is likely that the breach could risk the physical or non-physical safety of an individual including (but not limited to) the risk of discrimination, identity theft or fraud, financial loss and damage to reputation. A breach involving business information will be likely to have financial, legal or significant reputational impact on SFC as an organisation.
The below table provides an overview for assigning risk levels to incidents however each incident must be assessed on an individual basis.

Risk level	Risk level indicators	Examples
Low	- small quantities of business or personal information - Non-sensitive information - Information not breached into the public domain - Negligible consequences for the organisation or individual's involved	- An email containing no sensitive information is sent to a member of staff in error - An email containing train tickets sent to the wrong member of staff - Notes from a non-sensitive meeting left on a printer
Moderate	- Limited volume of non-sensitive personal information breached externally - Incident which risks sensitive information being released into public domain - Low level business information sent externally which is not for release - Some reputational damage to SFC possible - Inconvenience or annoyance to individuals concerned	- An email sent to members of the public is sent with all email addresses visible to recipients - Draft strategy document published on SFC website with staff comments and feedback still included - Member of staff sent another member of staff's payslip in error (no bank details)
High	- Presents a risk to the rights and freedoms of individuals - Special category personal data breached into the public domain - Large quantities of personal data breached into the public domain - Individuals involved in the incident may need to be notified of a breach of their information - Commercially sensitive information likely to cause significant reputational damage or damage working SFC's working relationships with third parties - Deletion of vital organisational records	- SFC systems accessed by an unauthorised third party - SFC laptop left on public transport and not recovered - Spreadsheets containing equalities information of students emailed to an unauthorised individual - Notes from sensitive SMT discussions about the future of the organisation released to the public - Staff HR records disposed of in non-secure manner - Live tender submission from a third party published on SFC website in error - Job applicants' equality monitoring forms left on public transport - Bank details breached into the public domain - Breach of SFC's IT systems' security