**St Georges, University of London (SGUL)**

**Confidential Data Incident Investigation Process**

1. **Introduction**
   1. The University recognises the importance in ensuring security around the processing of confidential data and has in place appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to confidential data.
   2. This document sets out the confidential data incident investigation process in the event a confidential data incident does occur. Note: any data incident involving personal data must follow the University’s Personal Data Incident Investigation Process.
2. **Confidential Data Incidents**
   1. All confidential data incidents are reported to the Head of Information Governance (HIG) via the data incident form found on [the website](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/policies-and-procedures/information-technical-security) or directly emailed. An incident number will be generated by the HIG who will identify an IAO to take the lead on investigating the breach. The IAO may assign a senior manager to carry-out the investigation on their behalf.
   2. Confidential data incidents will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers.
   3. The assigned officer is to consider the following:

* Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise.
* This could be isolating or closing a compromised section of the network, finding a lost piece of equipment/data or simply changing the access permissions.
* Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
* As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
* Where appropriate, in consultation with the HIG and SIRO, inform the police.
  1. Serious Incidents will be overseen the HIG who will escalate to the Senior Information Risk Owner as needed.

1. **Investigation**
   1. The assigned officer has 10 days in which to complete a data breach investigation report, unless notified any differently, and is to determine the circumstances below for all incidents:

* What data has been compromised
* Whether it has been inappropriately accessed
* How the incident can be contained (limiting or restricting further impact of the incident)
* The risk to the University
* How associated areas will be told, or ‘notified’ of the incident
* How the incident occurred
* Check weaknesses in SGUL processes or procedure which may have led to the incident and what corrective action is required to prevent reoccurrence, this may include:
* Training
* Guidance
* Disciplinary, and
* Process or guidance that needs to be modified.

1. **Assessing the Risk**
   1. Before deciding on what steps are necessary to put in place immediate containment the IAO lead is to assess the risks which may be associated with the incident. Perhaps most important is an assessment of potential adverse consequences for the university (this includes staff and students), how serious or substantial these are and how likely they are to happen.
   2. The following points are also likely to be helpful in making this assessment:

* What type of data is involved?
* How sensitive is it?
  + Remember that some data is sensitive because of its very nature (important research records) while other data types are sensitive because of what might happen if it is misused (financial or governance records)
* If data has been lost or stolen, are there any protections in place such as encryption?
  + What has happened to the data?
  + If data has been stolen, it could be used for purposes which are harmful to the University; if it has been damaged, this poses a different type and level of risk
  + Regardless of what has happened to the data, what could the data tell a third party about the University?
  + Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of e.g. a research project.
* What quantity of data is affected by the incident? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
* Who are the individuals involved in the data incident breached?
  + Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
* What harm can come to the University?
  + Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of the University?
* Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service the University provides?

1. **Response to the incident**
   1. The assigned officer is to, in agreement with their IAO, implement an action plan which will address the following factors, listed in priority order:

* Impact on the University or research project
* Impact on normal business operations
* Damage to the University’s reputation
* Prevention of any similar incident
* Recovery of stolen assets
* Disciplining or prosecution of the person or people responsible

1. **Notification of breaches**
   1. Informing the University and organisations that you have experienced a confidential data incident is an important element in breach management. However, informing about an incident is not an end in itself. Notification should have a clear purpose, whether this is to enable the University to take steps to protect itself or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.
   2. Answering the following questions will assist investigating manager in advising the IAO whether to notify any regulatory agencies:

* Are there any legal or contractual requirements?
* Can notification help you meet your security obligations with regard to protecting confidential data?
* Can notification help the University?
* Bearing in mind the potential effects of the incident, could the University act on the information you provide to mitigate risks, for example changing a password?
* Consider how notification can be made to regulatory agencies.
* Have you considered the dangers of ‘over notifying’. Not every incident will warrant notification so this requires serious consideration.
  1. The IAO will also need to consider who to notify, what they are going to tell them and how they are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to their decision:
* Make sure the appropriate regulatory body is notified. A sector specific regulator may require you to notify them of any type of breach.
* There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation
* The notification should at the very least include a description of how and when the incident occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the incident.
* When notifying organisations give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them
* Provide a way in which they can contact the University for further information or to ask questions about what has occurred – this could be a helpline number or a web page, for example.
  1. If informing the media, it is useful to inform them whether the University have contacted any regulatory agencies and what action is being taken.
  2. Also consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to the University, and trade unions.

1. **Post event reporting**
   1. The IAO will report on the findings to the Information Governance Steering Group.
   2. The SIRO may request the risk is be added to the University Risk Register.
   3. The SIRO, in conjunction with the HIG and Head of IT Services, will analyse the risk to the affected system or process and list the actions to mitigate the risk together with a date for the estimated completion date.
   4. Any risk that is deemed to be high should be reported to the Executive Board and Dir Governance, Legal & Assurance Services
2. **Evaluation and response**
   1. It is important not only to investigate the causes of the incident but also to evaluate the effectiveness of the response to it. Clearly, if the incident was caused, even in part, by systemic and ongoing problems, then simply containing the incident and continuing ‘business as usual’ is not acceptable; similarly, if the University’s response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.
   2. If it is found that existing procedures could lead to another incident then appropriate IAO will need to identify where improvements can be made. The following points will assist:

* Make sure you know what confidential data is held and where and how it is stored. Dealing with a confidential data incident is much easier if you know which data are involved.
* Establish where the biggest risks lie. For example, how much confidential data do you hold? Do you store data across the business or is it concentrated in one location?
* Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
* Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
* Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
* Consider whether you need to establish a group of technical and nontechnical staff who discuss ‘what if’ scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions

1. **Learning from Personal Data Incidents**
   1. To learn from incidents and improve the response process then incidents, where appropriate, are to be recorded and a Post Incident Review conducted. The following details are to be retained:

* Types of incidents.
* Volumes of incidents and malfunctions.
* Costs incurred during the incidents.
* The information will be collated and reviewed on a regular basis by HIG and any patterns or trends identified.