UNIVERSITY OF GIBRALTAR

# Data Security Breach Incident Management Policy

# Data Security Breach Incident Management Policy

Contents



| | |
|---|---|
| Date approved by University Executive | 18 January 2019 |
| Date approved by Board of Governors | 22 January 2019 |
| Date of (next) review | 22 January 2020 |

## 1. Background

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. The University needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

## 2. Aim

The aim of this policy is to standardise the University-wide response to any reported data breach incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents it aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of University management are involved in response management
- incidents are recorded and documented
- the impact of the incidents is understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

## 3. Definition

A data security breach is considered to be “any loss of, or unauthorised access to, University data”. Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential University Data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

## 4. Scope

This University-wide policy applies to all University information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the University. It is to be read in conjunction with the University Security Policy and Data Protection Policy.

## 5. Responsibilities

5.1 Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

5.2 Directors/Heads of School/Department

Directors/Heads of Departments and School are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

5.3 Lead Responsible Officers

Lead responsible officers will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

5.4 Contact Details

In the event that the Incident Management Team need to be contacted, contact details are as follows;

DPO ext. 816

Information Compliance Team ext. 806/807

ICT Helpdesk ext.810

**6. Data Classification**

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the University is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following approved University Data Categories:

6.1 Public Data:

Information intended for public use, or information which can be made public without any negative impact for the University.

6.2 Internal Data:

Information regarding the day-to-day business and academic operations of the University. Primarily for staff and student use, though some information may be useful to third parties who work with the University.

6.3 Confidential Data:

Information of a more sensitive nature for the business and academic operations of the University, or that could cause significant damage or distress to individuals, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the University.

6.4 Highly Confidential Data:

Information that, if released, will cause significant damage to the University's business activities or reputation, or would lead to breach of the Data Protection Act 2004. Access to this information should be highly restricted.

**7. Data Security Breach Reporting**

Confirmed or suspected data security breaches should be reported promptly to the IT Helpdesk as the primary point of contact on ext.810 email: ithelpdesk@unigib.edu.gi. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process. **See Appendix 1**.

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer to lead should be. **See Appendix 2**.

All data security breaches will be centrally logged by the IT Team to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

**8. Data Breach Management Plan**

The management response to any reported data security breach will involve the following four elements. **See Appendix 3** for suggested checklist.

A. Containment and Recovery

B. Assessment of Risks

C. Consideration of Further Notification

D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist for Data Security Breaches. An activity log recording the timeline of the incident management should also be completed. **See Appendix 4.**

**9. Authority**

Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

**10. Review**

The Information Compliance team will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

11. References: GRA:

https://www.gra.gi/gdpr-8-guidance-on-personal-data-breach-notification

**Appendix 1: Incident Report Form**

| | |
|---|---|
| Description of the Data Breach: | |
| Time and Date breach was identified and by whom: | |
| Who is reporting the breach: Name/ Post/ Dept | |
| Contact details: Telephone/ email | |
| Classification of data breached (in accordance with University policy)<br>i. Public Data<br>ii. Internal Data<br>iii. Confidential Data<br>iv. Highly Confidential data | |
| Volume of data involved | |
| Confirmed or suspected breach? | |
| Is the breach contained or ongoing? | |
| If ongoing, what actions are being taken to recover the data? | |
| Who has been informed of the breach? | |
| Any other relevant information | |

Email form to the DPO:

dpo@unigib.edu.gi and call 20071000 ext.816

If the data breach involves IT systems ALSO simultaneously copy IT Helpdesk:

ithelpdesk@unigib.edu.gi and call ext.20071000 ext.810 Callers should advise that a Data Security Breach report form is being sent.

Received by:

Date/Time:

**Appendix 2: Evaluation of Incident Severity**

The severity of the incident will be assessed by the DPO with the assistance of the Information Compliance Team. Assessment would be made based upon the following criteria:

| **High Criticality: Major Incident** | **Contact:** |
|---|---|
| Highly Confidential/Confidential Data | Lead Responsible Officer:<br>To be determined by the Incident Management Team |
| Personal data breach involves > 1000 individuals | |
| External third party data involved | |
| Significant or irreversible consequences | Other relevant contacts:<br>Governance and Information Compliance<br>Internal senior managers as required<br>Contact external parties as required i.e. police/GRA/individuals impacted |
| Likely media coverage | |
| Immediate response required regardless of whether it is contained or not | |
| Requires significant response beyond normal operating procedures | |

| **Moderate Criticality: Serious Incident** | **Contact:** |
|---|---|
| Confidential Data | Lead Responsible officer:<br>Director/Head of School, Faculty or Department affected by the incident |
| Not contained within University | |
| Breach involves personal data of more than 100 individuals | Other relevant contacts:<br>Registrar<br>Chief Financial Officer<br>Head of External Relations<br>Governance and Information Compliance |
| Significant inconvenience will be experienced by individuals impacted | |
| Incident may not yet be contained | |
| Incident does not require immediate response | |
| Incident response may require notification to University's senior managers | |
| Low Criticality: Minor Incident | Contact: |
| Internal or Confidential Data | Lead Responsible Officer<br>Director/Head of School/Faculty or Department (May delegate responsibility to another appropriate senior member of staff) |
| Small number of individuals involved | |
| Risk to University low | Other relevant contacts:<br>IT Helpdesk to advise and lead on technical aspects of containment/recovery<br>Governance Team to follow up on policy procedures for managing personal data breaches |
| Inconvenience may be suffered by individuals impacted | |
| Loss of data is contained/encrypted | |
| Incident can be responded to during working hours | |
| Example: | |
| Email sent to wrong recipient | |
| Loss of encrypted mobile device | |

**Appendix 3: Data Breach Checklists**

A. Containment and Recovery

B. Assessment of Risks

C. Consideration of Further Notification

D. Evaluation and Response

| Step | Action | Notes<br>(NB This Checklist is principally focused on IT related data breaches) |
|---|---|---|
| **A** | **Containment and Recovery** | **To contain any breach, to limit further damage as far as possible and to seek to recover any lost data** |
| 1 | IT Helpdesk - or ICT Director if out of hours - to ascertain the severity of the breach and determine if any personal data is involved | See Appendix 2 |
| 2 | IT Helpdesk – or ICT Director if out of hours - to identify Lead Responsible Officer for investigating breach and forward a copy of the Incident Report Form | To oversee full investigation and produce report for DPO /Information Compliance team. Ensure lead has appropriate resources including sufficient time and authority. If personal data has been breached must contact DPO urgently. In the event that the breach is severe, the DPO will lead the initial response. |
| 3 | Identify the cause of the breach and whether the breach has been contained?<br><br>Ensure that any possibility of further data loss is removed or mitigated as far as possible | Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process.<br><br>This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident. |
| 4 | Determine whether anything can be done to recover any losses and limit any damage that may be caused | E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups. |
| 5 | Where appropriate, the Lead Responsible Officer or nominee to inform the police | E.g. stolen property, fraudulent activity, criminal offence. |
| 6 | Ensure all key actions and decisions are logged and recorded on the timeline | |

| Step | Action | Notes |
|---|---|---|
| **B** | **Assessment of Risks** | **To identify and assess the ongoing risks that may be associated with the breach** |
| 7 | What type and volume of data is involved? | Data Classification/volume of individual data etc. |
| 8 | How sensitive is the data? | Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details). |
| 9 | What has happened to the data? | E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk. |
| 10 | If the data was lost/stolen, were there any protections in place to prevent access/misuse? | E.g. encryption of data/device. |
| 11 | If the data was damaged/ corrupted /lost, were there protections in place to mitigate the impact of the loss? | E.g. back-up tapes/copies. |
| 12 | How many individuals' personal data are affected by breach? | |
| 13 | Who are the individuals whose data has been compromised? | Students, applicants, staff, customers, clients or suppliers? |
| 14 | What could the data tell a third party about the individual? Could it be misused? | Consider this regardless of what has happened to the data. 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 other people. |
| 15 | Is there actual/potential harm that could come to any individuals? | E.g. are there risks to:<br>• physical safety;<br>• emotional wellbeing;<br>• reputation;<br>• finances;<br>• identify (theft/fraud from release of non-public identifiers);<br>• or a combination of these and other private aspects of their life? |
| 16 | Are there wider consequences to consider? | E.g. a risk to public health or loss of public confidence in an important service we provide? |
| 17 | Are there others who might advise on risks/courses of action? | E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use. |

| Step | Action | Notes<br>**(NB DPO/ Information Compliance team should lead on the below actions, working in conjunction with the department affected by the breach)** |
|---|---|---|
| **C** | **Consideration of Further Notification** | **Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions** |
| 18 | Are there any legal, contractual or regulatory requirements to notify? | E.g. terms of funding; contractual obligations. |
| 19 | Can notification help the University meet its security obligations under the seventh data protection principle? | E.g. prevent any unauthorised access, use or damage to the information or loss of it. |
| 20 | Can notification help the individual? | Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)? |
| 21 | If a large number of people are affected, or there are very serious consequences, inform the GRA (through the DPO) | Contact and liaise with the Governance and Information Compliance Team. |
| 22 | Consider the dangers of 'over notifying' | Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work". |
| 23 | Consider whom to notify, what you will tell them and how you will communicate the message | • 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.<br>• Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach.<br>• When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them.<br>• Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page). |
| 24 | Consult the GRA/ICO guidance on when and how to notify it about breaches | Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the GRA where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Any decision to report to GRA must be taken by or confirmed with DPO/ Information Compliance team who will liaise with GRA as appropriate. |

| | | |
|---|---|---|
| | | Guidance available from<br>http://www.ico.gov.uk/<br>for_organisations/data_protection/<br>the_guide/principle_7.aspx<br><br>https://www.gra.gi/gdpr-8-guidance-on-personal-data-breach-notification |
| 25 | Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals | E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies. |

| **Step** | **Action** | **Notes**<br>**(NB DPO/ Information Compliance team should lead on the below actions, working in conjunction with the department affected by the breach)** |
|---|---|---|
| **D** | **Evaluation and Response** | **To evaluate the effectiveness of the University's response to the breach** |
| 26 | Establish where any present or future risks lie | |
| 27 | Consider the data and contexts involved | E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept. |
| 28 | Consider and identify any weak points in existing security measures and procedures | E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections. |
| 29 | Consider and identify any weak points in levels of security awareness/training | Fill any gaps through training or tailored advice. |
| 30 | Report on findings and implement recommendations | Report for DPO/ Information Compliance teamwho will consider further reporting that may be required. |

**Appendix 4: Timeline of Incident Management**

| Date | Time | Activity | Decision | Authority |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |