Botho University
Information Governance and Management Policy

1 Background

1.1 Botho University is committed to protecting the privacy and security of personal information and personal data.

1.2 As a Data Controller, Botho University is responsible for how personal data collected from staff, students, contractors, alumni, and any other person is held, processed, and used.

1.3 In order to fully comply with Data Protection legislation the University is required to have in place a clear approach for managing data breaches across the University. In order to ensure best practice, the University has put in place a robust and systematic process for responding to any reported data breach.

2 Purpose of this policy

2.1 The purpose of this policy is to set out the procedure to be followed to ensure a consistent and effective approach to managing data breach and information security incidents across the University.

2.2 This policy relates to all personal and special categories of data held by the University regardless of format and applies to all staff and students at the University and any individual who processes University Data. This includes, management, staff, contractors, temporary staff, consultants, and data processors working for or on behalf of the University.

2.3 This policy provides clear lines of responsibility so that individuals are aware of who to contact in the event of a data breach.

2.4 In following the procedure set out in this policy the University aims to:

2.4.1 Quickly identify when a Data Breach has occurred;

2.4.2 Ensure that any breach is promptly contained;

2.4.3 Minimise the risk associated with any breach;

2.4.4 Determine what action is appropriate in light of any Data Breach;

2.4.5 Ensure that relevant people have been notified promptly of any breach;

2.4.6 Give consideration to what can be done to prevent similar breach events from happening in future.

3 What is a Data Breach

3.1 A Data Breach in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the University's information assets and/or reputation.

3.2 Data Breaches include both confirmed events as well as suspected and near misses which could potentially lead to the loss of personal data, but which in the circumstances has not.

3.3 The following is a list of examples of Data Breaches:

3.3.1 a hacker attacking our web server resulting in access to Personal Data;

3.3.2 accidental loss or theft of equipment (laptop, tablet, phone, memory stick) on which personal data is stored;

3.3.3 System failure;

3.3.4 theft of personal data from a filing cabinet or loss of hard copy files or documents containing personal data;

3.3.5 unauthorised use of systems containing personal data;

3.3.6 unauthorised access to or modification of data or information systems;

3.3.7 unauthorised disclosure of confidential information;

3.3.8 human error resulting in loss, release or transfer of Personal Data; and

3.3.9 where Personal Data is transferred by someone deceiving the organisation into thinking they are someone authorised to receive the information .

This is not an exhaustive list and there may be other events which require escalation. If in doubt, please defer to the University's Data Protection Officer (DPO).

4 What should I do if I suspect there may be a Data Breach?

4.1 If a data breach has occurred it must be reported to the Data Protection Officer within 24hrs.

4.2 Any individual with access to the University's information who becomes aware of a data breach is responsible for ensuring that the matter is reported immediately to the Data Protection Officer as per the requirements of the University's data breach reporting procedure. (Link to form). Staff members must report to their immediate supervisor, the respective Dean (as per the University's organisation structure) and the Data Protection Officer. Contact details of the Data Protection Officer is dpo@bothouniversity.ac.bw. This position is managed by the Office of the Vice-Chancellor.

4.3 The individual must include full and accurate details of the event, including when the breach occurred (date and time), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

4.4 The individual reporting breach should rely on the DPO who has specialist skills and knowledge to go through the process of identifying how serious the data breach is, whether there is a need to report it to the Information and Data Protection Commissioner's office, and what action needs to be taken in light of the data breach.

4.5 What can sometimes look like a small event can escalate very quickly to become a data breach if allowed to continue unchecked. The longer a data breach goes unreported, the longer a vulnerability may remain unaddressed allowing an incident to escalate or further incidents to occur.

4.6 If the data breach arises out of office hours, it must be reported as soon as practicable, but not later than the next working day.

4.7 All students and staff should be aware that failure to act in accordance with this policy may result in the University's disciplinary procedures being instigated.

5 What happens after a Data Breach is reported

5.1 The DPO supported by members of the Office of Vice Chancellor will firstly determine whether or not the data breach is ongoing. If so, steps will be taken immediately to contain and minimise its effects. The DPO will also determine who may need to be notified as part of the containment, and whether or not to inform the police.

5.2 DPO will make an initial assessment to establish the severity of the data breach and will reach a decision whether or not to inform the Information and Data Protection Commissioner's office. A notification needs to be made to the Information and Data Protection Commissioner's office within 72 hours.

5.3 Every incident will be considered on a case by case basis, taking into account the following:

5.3.1 Whether the breach is likely to result in a risk of adversely affecting a natural person's rights and freedoms (test for notification to Information and Data Protection Commissioner's office by DPO);

5.3.2 Whether or not the breach is likely to result in a high risk to the rights and freedoms of natural persons (test for notifying data subject by DPO);

5.3.3 Whether notification would assist the individual(s) affected e.g. to mitigate risks;

5.3.4 Whether notification would help prevent the unauthorised or unlawful use of personal data;

5.3.5 The dangers of over notifying, recognising that not all cases warrant notification and being mindful not to cause disproportionate work unnecessarily.

5.4 All Data Breaches will be assessed by reference to the risk the data breach presents to the University and to the individuals whose data is affected.

5.5 The DPO will then carry out a full investigation into the circumstances leading to the Data Breach and establish whether, in the case of a breach, anything can be done to recover any losses and limit the damage. An investigation will consider the following:

5.5.1 the type of data involved;

5.5.2 its sensitivity;

5.5.3 the protections in place (e.g. encryptions);

5.5.4 what has happened to the data (e.g. has it been lost or stolen);

5.5.5 whether the data could be put to any illegal or inappropriate use;

5.5.6 data subjects affected by the breach, number of individuals involved and the potential impact on them;

5.5.7 whether there are wider consequences to the breach.

5.6 Once the Data Breach has been contained and the breach or incident has been resolved, the Data Protection Officer will prepare a Data Protection Report on any findings and will make recommendations as to what action is to be taken in order to ensure no similar incident reoccurs in the future. The DPO will liaise as appropriate with the Commissioner's office.

5.7 No steps should be taken by staff or students or any third party without consultation and agreement of the DPO.

6 Communications

6.1 The DPO will liaise as necessary with the communications team at the University in relation to making any announcements to the press and in consultation with the ICO will determine if individuals affected by the breach should be contacted.

6.2 Any phone calls or emails received relating to the Data Breach must be forwarded to the DPO immediately.

6.3 A record will be made of all personal data incidents whether or not they are determined to be a breach.

7 Evaluation and response

7.1 At the end of any incident response which has necessitated a report to the Information and Data Protection Commissioner's office , the DPO will carry out a review of the effectiveness of the response and whether any changes to the policy and procedure set out above are necessary.

7.2 This policy will be updated as necessary to reflect best practice and to ensure compliance with any legislative changes.