DATA SECURITY POLICY AND PROCEDURES

Policy Number:		**Version:**	1
Drafted by:	Student (Melissa)	**Board approval on:**	November 2022
Responsible Person:	Strategic Finance Executive	**Scheduled Review Date:**	November 2023

INTRODUCTION

Big Yellow Umbrella (BYU) continues to promote ethical practice and are committed to achieving and maintain a strong information security culture across the provision of its services. BYU recognises that is the responsibility of the organisation in protecting confidential data in compliance with government laws, policies, and regulations, as well as reviewing data and security risks regularly.

This document is to be applied to:

- The provision of all services
- The provision of client information
- The use of electronic devices, online databases, and all other forms of communication

PURPOSE

It is important for organisations to have strategies in place to protect the confidential information of employees, service users, and programs delivered. The Australian Cyber Security Centre (ACSC) recommends a plan to be implemented for all users and computers storing sensitive information. This is to help organisations protect themselves against data breaches, cyber threats, and leaking of private information. Recognising the confidentiality, privacy and personal security of all stakeholders involved in the organisation, BYU aims at promoting the highest quality of security measures.

BYU continues to maintain security through:

- Employing an I.T. Specialist Service to provide adequate protection, support and assistance surrounding data security
- Ensuring data collection and data storage processes are up to date and monitored across all staff, students, and volunteers
- Providing sufficient training on how to best reduce the risk of cyber attacks

POLICIES

Committed to employees, volunteers, students, and service users, in protecting confidential information, BYU will establish, maintain, enforce, and continually improve policies, procedures and safeguards to protect the personal and confidential data held in electronic and physical files against unauthorised access, use, disclosure, destruction, loss and alteration.

ROLES AND RESPONSIBILITIES

The Chief Operations Manager and the Strategic Finance Executive are responsible for the implementation and monitoring of all aspects of this data security policy.

All staff, students and volunteers are responsible for adhering to this policy internally and externally.

The staff, students and volunteers are responsible to notify the Chief Operations Manager and the Strategic Finance Executive of all complaints and any other updates in team meetings.

Staff are to identify and report any gaps in security or incidents of security breaches relating to confidential information to the Chief Operations Manager and the Strategic Finance Executive.

PROCEDURES

Password Management

BYU recognises the importance of creating secure passwords, regularly changing passwords, and engaging in secure communication and storage of passwords. I.T Specialist Service have been employed by BYU to provide adequate support and consistent procedures around the use of passwords across all electronics and emails, including the implementation of a two-factor authentication for an extra layer of security.

Procedures around password resets are as follows:

1. Users to request password reset or access change directly to Chief Operations Manager and the Strategic Finance Executive's email.
2. Management to approve and forward ticket onto I.T Specialist Service employed by BYU
3. I.T. Specialist Service to action and reset password and send to mobile number on record.
4. I.T. Specialist Service to action and provide notification that access has been granted via the ticket logged from Step2

Storing Client Files

Saving client intake forms received across BYU services and programs are to follow strict guidelines in accordance with DCJ requirements. Client information is to be collected using a paper intake form, and personal information is to be directly added to the DS system once consent is received to store their data on the database. A scanned copy of this form is then to be uploaded to the client's online DS profile. Once uploaded the intake form is to be shredded. This form will be stored along with regular backups for the required 7 years.

Cyber Security

Cyber security is maintained throughout BYU by employing an I.T Specialist Service. This I.T Specialist Service will provide up to date and comprehensive security measures across all electronic devices used by the organisation including regular changes of passwords, backups for BYU, as well as instructions and training around protecting devices and files from cyber threats.

BYU staff, volunteers, and students are to be prepared, informed, and alerted of the dangers and warning signs of cyber threats including:

- 'phishing' which refers to suspicious emails, calls, or messaged devised to gain access to personal information, sensitive data, and money from recipients.
- Malicious software (malware) which is a type of software that is designed to damage and disrupt a computer or server or gain unauthorised access to information. It includes viruses, Trojans, spyware, and worms.

Situational Awareness

When working remotely, staff, student, and volunteers must take appropriate measures to ensure they are connected to a trusted network and protect the confidentiality of information they are using. To avoid risks associated with human errors, all employees are to take responsibility when handling private information, to make sure it stays private.

Role of Employees

- If any personal passwords require changing, notify management immediately so it may be recorded and determined to be safe
- Practice protective measures in response to cyber threats such as not opening suspicious attachments or clicking on suspicious links, and looking out for unexpected attachments, requests to provide login credentials, requests for money or changes to bank accounts
- Do not send sensitive information unless it is necessary. If you do need to send sensitive information to someone else, always check the email addresses of recipients to confirm you are sending the information to the right person
- When using email, be mindful of accidentally clicking 'reply all' to emails, consider the contents of the email chain and remove anything that doesn't need to be shared when forwarding emails onto new participants, and check email attachments for confidential information before sending
- Reduce the risk of human error by taking responsibility and care when handling private information, to make sure it stays private
- Keep devices updated and turn on automatic updates
- When working remotely, staff are to limit file sharing, only login to sites if they are secure, and be cognisant of the people around them so that screens are not seen when entering sensitive information
- Commit to restricting 'tailgaters' by ensuring doors to secured areas are closed immediately. If someone asks to borrow your access card to get into the office, do not give it to them. If a suspicious or unfamiliar person has been seen loitering around an access control point or following a staff member or someone else through an access control point without visible identification, they are to be challenged if it is safe to do so. Otherwise, they are to be immediately reported to management or anyone else on site that you feel might be able to assist you in this circumstance
- Close down computers when not in use and turn over client files and sensitive information to ensure they are not visible to others who do not need to see the content
- Do not leave client information or any other sensitive information open on desks at the end of day to protect from cleaners who may enter
- Do not share or discuss any personal client information unless consent from the client has been received and the conversation is in the best interest of the client
- Ensure all confidential filing cabinets remain locked when not in use

Role of Managers

- If BYU detects an actual or suspected information security incident, DCJ is to be notified and kept informed of progress until its resolution. Investigate the information security incident and notify DCJ of early findings
- Ensure that client information storage processes are consistent across all staff throughout all programs and services delivered by BYU
- Maintain Cyber Security Insurance
- Provide regular and up to date staff security training and information sharing to ensure that all are informed on the procedure surrounding password rests and cyberthreats

RELATED DOCUMENTS
Clients Record Policy
Code of Conduct Policy
Confidentiality and Declaration Policy
Customer Service Policy
Cyber Security Centre: Recognise and report scams | Cyber.gov.au
DCJ Website
Disclosure of Information Policy
Financial Management Policy
Fraud Management Policy
Governance Policy
Privacy Policy
Risk Management Policy
Social Media Policy
Staff Induction Policy
Standards of Practice Guidelines Policy

AUTHORISATION

The Board of Big Yellow Umbrella have reviewed and approved this policy

Signature of Board Secretary: ________________________________

Date of approval by the Board: ________________________________

On behalf of the Big Yellow Umbrella