# Fortify Backup Process Draft

This document is a draft of the process that will undertake between a client (organisation) and Fortify when implementing backup services to a client. The purpose of this is to clarify the basic and technical processes from first contact to final feedback of any given backup specific scenario.

# User Case - Example of where your organization may require Fortify’s backup advisory service

You have been asked by your organisation’s Audit & Risk Committee to provide a report on the status of the backup systems and the ability to recover the business in case of a major disaster such as being exposed to a ransomware attack.

You think your IT person is performing basic backup services but there are no reports generated and there are no guarantees that the backed-up data is accurate or that all your critical data has been backed up. To add to your woes your IT provider cannot supply information on whether the backups have been tested or if your backup data will not be affected during an attack where adversaries attempt to encrypt all systems.

You need to get professional assistance to solve the critical parts of the backup as described above, but it sounds expensive and being a small not-for-profit organization, you have a very limited budget to get this done. You are also not aware of whom to approach and how to go on about engaging a consultant to help you achieve what is required.

# Process Step guide

## Get started steps

The first 9 steps of this guide are a baseline process which all new / current clients are required to undertake (current / reoccurring clients skip to step 6).

1. Client will navigate to newly developed Fortify website – [www.Fortify.com.au](http://www.Fortify.com.au)
2. Client is required to create an account and register their organisation into our system
3. Client is required to read and accept guidelines / terms and conditions regarding process and storage of personal / sensitive data.
4. Client is required to read and complete a self-assessment questionnaire based on their current cybersecurity maturity level process within the organisation. (if assistance is required, a chatbot will be available).
5. Once assessment is complete and submitted, the results are stored securely within Fortify for when the client is ready to submit / create a job ticket.
6. Client selects to create a job ticket and is presented with an array of user cases (these are example cases to help educate clients and to give better understanding of their own situation).
7. Client is required to give a short description of their situation and what they may require from Fortify (an automated email is sent to the client as a job confirmation and to notify ticket is active).
8. Client will be contacted within 24 hours by a cybersecurity professional volunteer who has been specifically selected for that client’s job ticket based on self-assessment results and client description.
9. Client and volunteer will conduct Fortify standard practices to reach a resolution of the client’s problem based on the client description.

## Client / Volunteer Interaction

The volunteer will be automatically matched based off questionnaire / description results. In this case the client / organisation lacks back procedures, knowledge, and experience, therefore a cybersecurity expert that specialises in data backup has been matched with the client.

1. Successful connection is made between client and volunteer.
2. Client gives detailed run down on scenario explaining only basic backup services are in place with no status reports / updates.
3. Volunteer revises client’s self-assessment questionnaire specifically highlighting backups. From this the volunteer can confirm and gauge the knowledge level of the client and proceeds to provide options in a user-friendly manner
4. Volunteer highlights recommendations / procedures that should be implemented for the client to improve their security / data security and structure. (Volunteer can create a checklist (this can be based off the questionnaire)) eg:

* Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.
* Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.
* All privilege level accounts cannot access any/ all data backups.
* All privilege level accounts cannot modify or delete data backups.
* Build / Implementation of an up-to-date backup system:
  + Analyse
  + Register results
  + Select appropriate backup vendor and solution
  + Determine hardware / software requirements
  + Deploy and maintain backup system

1. Volunteer will revise / educate client in relation to backup options and possibilities:

* On-site, off-site, and cloud backups
* Automated audits for cloud backup strategy
* Third party vendors such as Microsoft Azure
  + Microsoft Azure backup and restore plan targeting ransomware. More information can be found here: <https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware>
  + Microsoft Azure immutable storage plan targeting data modification and deletion by unauthorised users / privilege levels. More information can be found here: <https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview>

1. Volunteer revises / concludes and provides a clear pathway for client to implement effective backup systematic solutions in-line with business goals and processes.
2. Client accepts contact is satisfactory and is comfortable with the information given, can implement a backup system.
3. Client may keep ticket active for another 24hours if assistance is needed, if not, client is required to end job ticket.
4. Contact between client and volunteer is terminated.
5. Client is given option to provide feedback regarding contact and performance.
6. Volunteer is required to complete an electronic job sheet to be stored with client’s profile.