IT Disaster Recovery Plan

Plan revision history

Revision	Date of revision	Name	Checked by	Signed
1	26/1/21	Peter See	Goh Soon Huat	

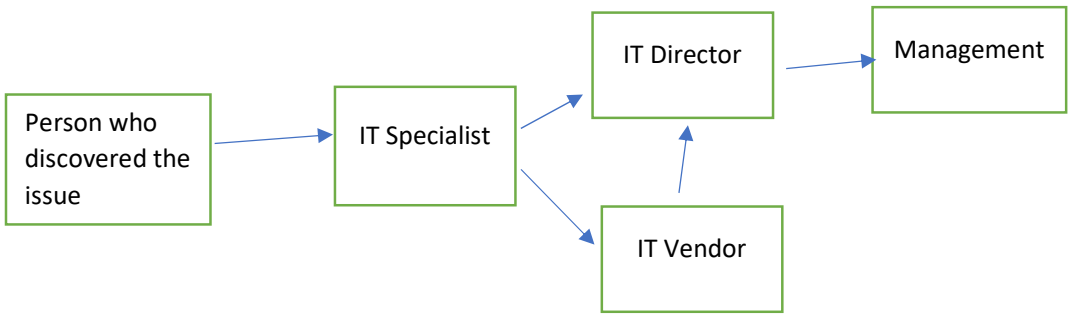
Key Personal Contacts

Name	Title	Contact mode	Details
Peter See	IT Specialist	Work	63758923
		Mobile phone	83825437
		Email address	ps@alpha.com.sg
		Alternate Email	shc@hotmail.com

Name	Title	Contact mode	Details
Goh Soon Huat	IT Director	Work	63758927
		Mobile phone	90092166
		Email address	gsh@alpha.com.sg
		Alternate Email	

Name	Title	Contact mode	Details
		Work	
		Mobile phone	
		Email address	
		Alternate Email	

Notification calling Tree



External Contacts

Name	Title	Contact mode	Details
Alex Chin	IT Vendor	Work	84485109
		Mobile phone	
		Email address	alex@terrabit.com
		Alternate Email	

Name	Title	Contact mode	Details
		Work	
		Mobile phone	
		Email address	
		Alternate Email	

Backup Strategy

Folders/ Applications	Backup strategy	Frequency
Deltek	Acronis backup to QNAP	Daily
Drawing folder	Acronis backup to QNAP	Daily
On premise exchange	Acronis backup to QNAP	Daily
Virtual machines	Acronis backup to QNAP	Weekly
Project Folder	Synology active backup	Daily
Email Archive	Backup to onedrive	weekly
Accounts/HR	Synology active backup	Daly
Zircon Database backup	Backup to Onedrive	Every 3 days
Admin folder	Synology active backup	Daily

Server Breakdown Recovery Procedure

1) User to inform IT Specialist regarding server issues.

2) IT Specialist to determine and pinpoint which server is having issue.

3) IT Specialist to assess the severity of the breakdown and the type of breakdown. (Hardware or software related)

4) IT Specialist to inform and provide IT Director regarding the specific information regarding the breakdown.

5) IT Specialist to source for new hardware or part replacement as per necessary.

6) IT Specialist to document down the incident in the service report form.

Ransomware Recovery Procedures

1) Upon infection, IT Specialist to locate the source of infection and remove the infected server/workstation from the network immediately.

2) IT Specialist to inform IT Director regarding the infection.

3) IT specialist to assess the damage of the infections, type of files infected and the how many servers are impacted.

4) IT Specialist to discuss with IT Director regarding course of actions and to decide if IT vendor activation is required or not.

5) IT Specialist to run virus scan on all servers to ensure clearance.

6) IT Specialist to proceed with file recovery process.
   i) To see if previous versions backup is affected or not. If not affected, recover back the affected files to the last known backup.
   ii) If previous version backup is affected, to use the Acronis or Synology backup copies as per necessary to restore back the affected files.
   iii) To delete off the infected files after doing file restoration

7) After files restoration are done, IT Specialist is to review the recovery process, assess the damage done such as amount of data lost and to investigate the cause of the infection.

8) IT Specialist to reformat the infected server before reconnecting back to network.

9) IT Specialist to document down the incident in the service report form.