CYBER SECURITY AND BCM
Work Remotely Checklist
2021

recoverdex

Ref.	Business Continuity	Status
BC01	Ensure all stakeholders are aware of your whereabouts	
BC02	Ensure proper and adequate network connectivity to office/core systems/disaster recovery site	
BC03	Ensure proper access levels to core systems and support systems	
BC04	Ensure proper testing and rehearsals were done prior to working remotely	
BC05	Maintain an escalation and notification list/system/application	
BC06	Have backup plans for working remotely (UPS/Gen-Set, WI-FI, printer, data)	
BC07	Keep Crisis Management Team (CMT) informed of any changes in work patterns	
BC08	Check-in regularly with Team/s	
BC09	Ensure all data, parcels, information is sent back securely to office/DR site	

Ref.	Cyber Security	Status
CS01	All data devices (laptops/mobile) must have hardware encryption	
CS02	Ask staff NOT to defer critical updates to software (be aware of scams)	
CS03	Confidentiality must be protected at all times (remind staff of this)	
CS04	Enforce strong password management (PKI/SSO)	
CS05	Make multi factor authentication (MFA) mandatory for all remote workers - Including email and when accessing any critical systems or applications	
CS06	Remind staff NOT to lend their machines to their children or other members of the family or friends	
CS07	Remind staff NOT to open links or documents with Coronavirus information unless it can be confirmed that it is from a reliable source. Ask them to report these.	
CS08	Remind staff that surfing porn, amongst other things, is illegal	
CS09	Staff must not visit sites like illegal movie websites as they pose a risk of ransomware and malware infection	
CS10	Stress the IMPORTANCE of NOT sharing passwords (remote working can lead to more password sharing)	
CS11	Use screen filters to make shoulder-surfing harder	
CS12	Set remote registry ACL	

Ref.	Phishing Emails	Status
PH01	Staff MUST report malware/ransomware infections immediately	
PH02	Remind staff that it's ok to make a mistake and that they should own up if they have, especially if they have: - Accidentally clicked on a suspicious file and or link - Opened a suspicious PDF or Word, Excel file with a macro	

Ref.	Online Communications	Status
OC01	Remind staff to MUTE the microphone when they are not speaking in a conference call	
OC02	Educate all staff to ensure webcams are blocked by default (make sure it is policy)	
OC03	Remind staff NOT to leave their machines UNLOCKED, especially during a call or when leaving their devices unattended	
OC04	Staff should NOT work from coffee shops or public places (if possible) – especially if they are on confidential calls or working on confidential documents	

Ref.	Governance	Status
GO01	Ensure that all respective policies are adapted to accommodate working remotely	

GO02	Ensure you are familiar and have consented to the following policies: - Code of Conduct - Work From Home/Remote Access - Acceptable Usage - Information Security - Logical Access Management - IT Governance - Business Continuity - Disaster Recovery - Incident Management - Change Management - Data Protection	
GO03	Ensure that all staff are aware of changes in policies and procedures	
GO04	Ensure all staff have access to all policies	

Ref.	Backups	Status
BK01	Provide staff software to ensure their critical documents are backed up	
BK02	Ask staff to back up their data on an approved external hard disk that is NOT permanently connected to the device	
BK03	Ask staff NOT to use approved external cloud storage services	
BK04	Ask staff to reach out to discuss any cloud storage or cloud service solution that they want to use	

Ref.	Privacy and Data Protection	Status
PR01	A clean desk policy should also be maintained at home	
PR02	Remind all staff of their responsibility to respect the privacy of your clients and your staff	
PR03	Remind IT and cybersecurity folks to be extra vigilant for possible malicious activity on user accounts	
PR04	Staff must be reminded NOT to email personal information via email OR store personal information in non-approved locations/devices	
PR05	Staff members must be very careful when sharing phone numbers and or emails. Ensure that this information is deleted as soon as possible	

Ref.	Cyber Security Attack and Response	Status
IR01	Constantly remind staff to be alert for phishing emails and other attempts to compromise/steal account and personal details	
IR02	All malicious activity and suspect emails must be reported immediately	
IR03	They should be encouraged to escalate to certain stakeholders if they want to	
IR04	Security staff must be extra vigilant and actively seek out suspicious activity (given the remote working habits of users this may be operationally expensive)	
IR05	Ask IT and security staff (including outsourcers) to pick up the phone and call if it's important rather than solely rely on email. (use a separate out-of-band app or something as simple (not very secure) as WhatsApp groups for urgent communications	
IR06	Keep a printed copy of your procedures and checklists at home AND make sure they ARE not easily accessible	
IR07	Remind all staff that it's ok to make mistakes (like sending emails to wrong recipients, clicking on a malicious link, causing an outage etc.) and that they MUST own up immediately. Stress that in most cases there will be NO repercussions	

Ref.	Privileged users:	Status
PA01	Ensure you inform all IT and business privileged users and: - Remind them of their responsibilities - Insist that they DO NOT login for DAILY tasks with high privileges - Demand that they REPORT all errors/confess to mistakes immediately	

Ref.	Exceptions	Status
EX01	Create a centralised "exceptions register"	
EX02	Ensure that this is controlled properly and reviewed regularly	
EX03	Have set policies to avoid everything being on the "exceptions list"	
EX04	Ensure that you have power surge and lightning protector plugs	