هيئة أبوظبي الرقمية

ABU DHABI DIGITAL AUTHORITY

Cyber Security Remote Working Checklist

OVERVIEW

Based on the government direction for employees to work from home through the Covid-19 epidemic, an increase dependency on information systems and technology on which information assets reside introduces new risks that must be identified in a timely manner and managed effectively. Information security requires active awareness and effective protection of the confidentiality, integrity and availability of information assets where ADGE's must adjust their information security program considering the current situation. Abu Dhabi Digital Authority has developed a checklist based on global best practices to have a safe remote working environment.

SCOPE AND APPLICABILITY

Control Standards defined within this document have applicability to Abu Dhabi government personnel, contractors and other third-party organizations with responsibility for the creation, handling, storage, transmission and destruction of Abu Dhabi government information assets, including information systems and other equipment.

ADGE's have the responsibility for ensuring that controls are deployed in sufficient depth and range to ensure effective management of risk.

CYBER SECURITY CHECKLIST

Awareness To Employees

An increasing day to day activities are done remotely by government employees which poses additional risks to ADGEs. To better help in preventing cyber-attacks; awareness massages should be send to employees through different channels to remind them of:

IT will **Not** call employees about password resets (to help avoid being scammed). ☐

Not to open links, documents, and maps with Coronavirus information or other phishing scams. ☐

Ensure employees are **aware** of important phone numbers and email addresses in case of an incident. ☐

Employees **must** report malware/ransomware infections immediately through official channels. ☐

Not use unapproved USB flash drives and unapproved cloud services. ☐

Ensure that Computers and terminals be **logged off** when not in use. ☐

Employees **must** ensure that sensitive communications cannot be read by unauthorized parties, including family members or visitors. ☐

- Employees **must not** share sensitive information via personal email or store government information in non-approved locations.
- Employees must use only **officially approved** conference apps considering:

  Having a password for every meeting or conference call where applicable.

  Ensure their meetings are not being recorded. If a meeting is being recorded, all participants should be aware.

  Remind employees to exit or close the app once the conference is complete.

CYBER SECURITY CHECKLIST

Controls To Be Implemented Where Applicable

RW.C.1	Ensure that support staff are on high alert and **challenge** password resets or 'strange' requests.	☐
RW.C.2	Ensure that **privileged** users do not login for daily tasks with high privileges.	☐
RW.C.3	Require all remote login (users and administrators) to be done over **secure** channels.	☐
RW.C.4	**Block** access to a machine (either remotely or locally) for administrator-level accounts.	☐
RW.C.5	All remote access connections should occur via a Virtual Private Network (**VPN**).	☐
RW.C.6	VPN connection **should** be established using either IPSec or SSL-based capabilities.	☐
RW.C.7	VPN client software/configurations should only be ones **approved** and provided by Entity's IT function	☐
RW.C.8	Remote access activity **logs** should be **reviewed** and analyzed regularly to identify any potential anomalies or suspicious activities.	☐

RW.C.9 Remote access gateways **should** only accept one connection per approved user account at any one time. ☐

RW.C.10 Set a **maximum** session time for logged on users for sensitive systems and applications. ☐

RW.C.11 Terminate **inactive** sessions after a predefined period of inactivity. ☐

RW.C.12 Deceives connected to the core network should be **scanned** regularly for viruses and malwares ☐

RW.C.13 Two factor authentication **should** be used to improve authentication mechanisms for remote access connections. ☐

RW.C.14 Ensure that **no** procedures are bypassed (no emergency change without approval etc). ☐

RW.C.15 Ensure to have a **clear** procedure to follow in case of a security incident and communicate to relevant parties. ☐