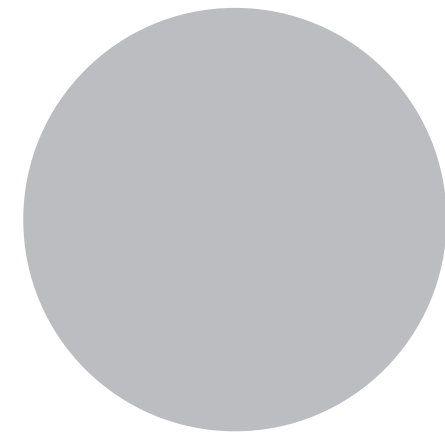
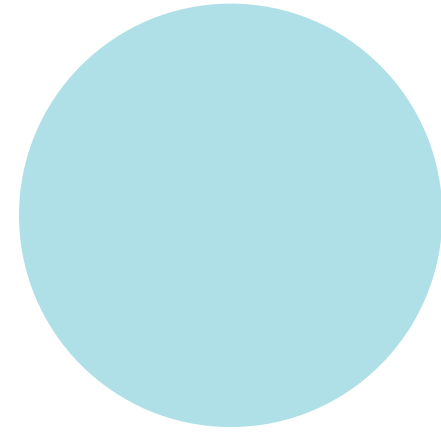


**01
Physical
Security**
An increased



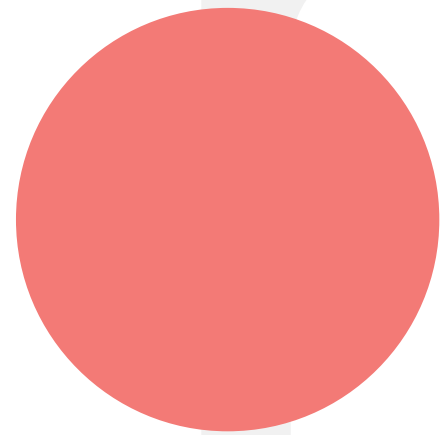
**02
Software
Patching**

Consider switching client device settings in the event of an extended work from home.



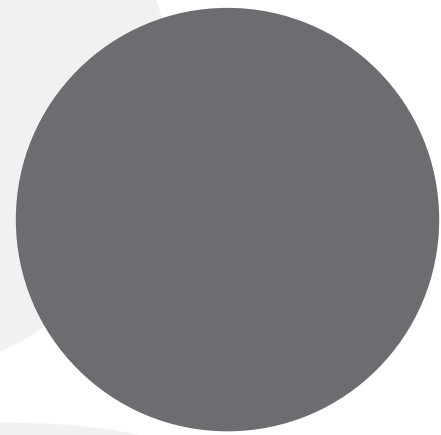
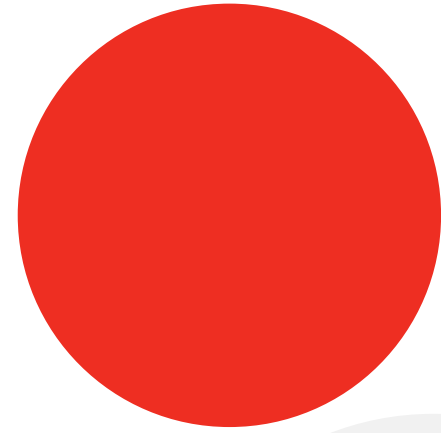
**03
Password**

Include display timeouts, lock screens, pin codes and or biometric security settings where that functionality is available.



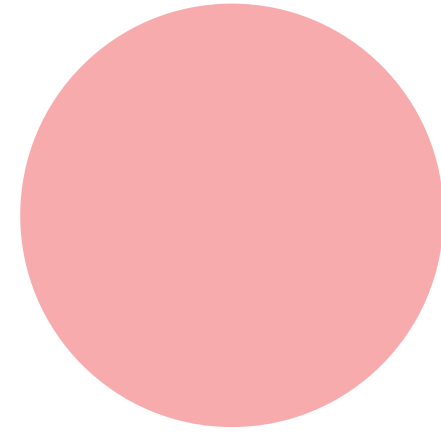
**05
Identity and
Privilege Access
Management**

The use of an identity provider is recommended which ensures a centralised management portal to administer users and to enable advanced security features such as multi-factor authentication, policy management, account and application provisioning and reporting.



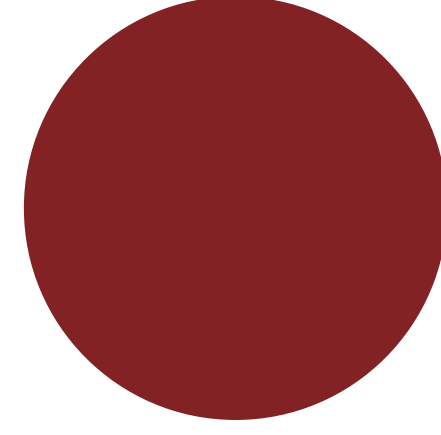
**06
Backup**

It is recommended that companies have a comprehensive data protection program in place to protect data irrespective of where it resides.



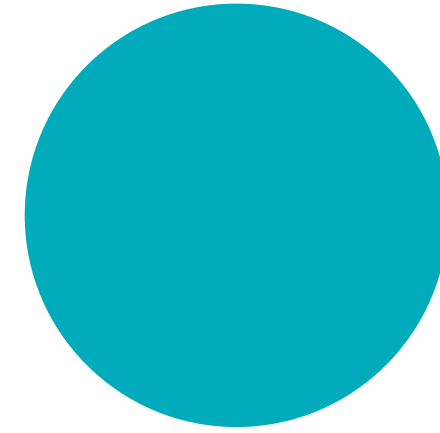
**07
Networking**

Users connectivity should be established to ensure they have both the speed and quality of connection to complete their working requirements.



**08
Attack**

Hovering over links to ascertain the validity of the address, not clicking on emails you're not familiar with and overall having a zero-trust view of internet originated traffic and communications holds.



**09
Hygiene**

Personal hygiene is particularly key as this moment in time for the team member working remotely but also the devices that they use.

