

# Reopening the office

## The cybersecurity and data protection essentials



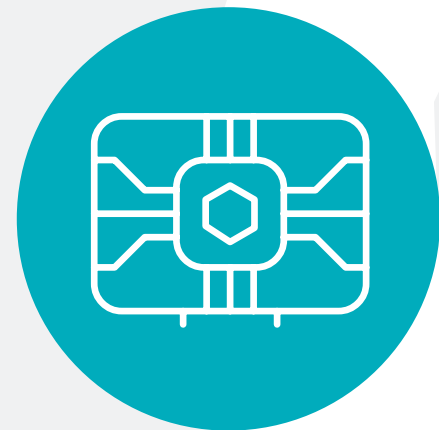
### 02 Data protection and privacy

Seek the advice of your Data Protection Officer or Privacy Officer on impact of changes made to existing processes or new processes where data is recorded and collated. Conduct Privacy Impact Assessments (PIAs) where relevant



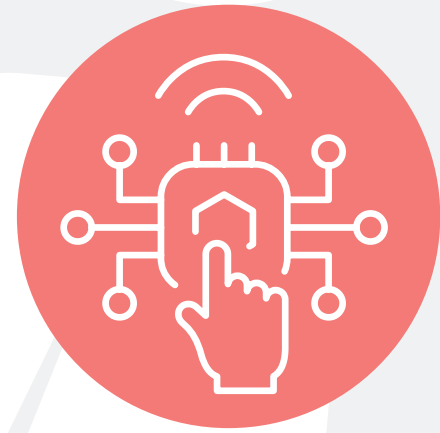
### 01 Physical security

Make sure that physical security controls, employee identification and physical media are all up to date and fully operable



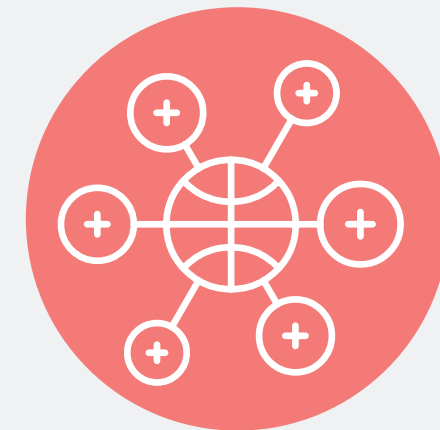
### 03 Asset management

Re-evaluate bring your own device (BYOD) policies and ensure that all non-inventoried assets are correctly logged



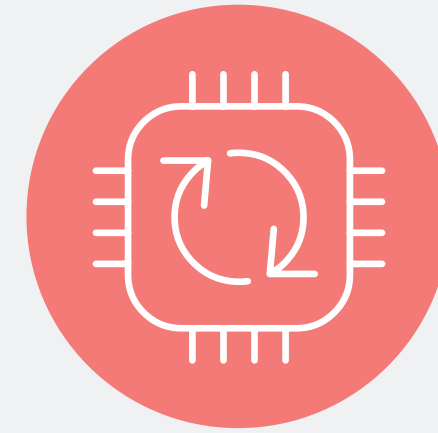
### 04 Access control

Ensure credentials like multi-factor authentication (MFA) and password expiration and reset are all up to date



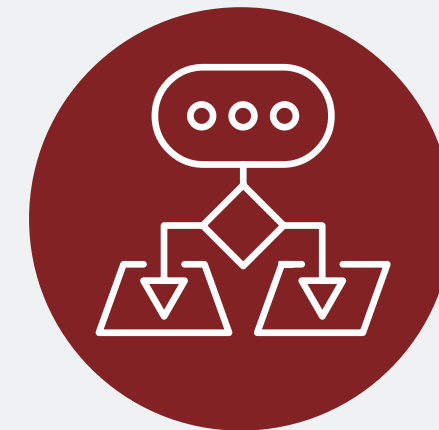
### 05 Network security

Remote access is still important during a phased return to work, so keep network services such as Virtual Private Networks (VPNs) available and secure



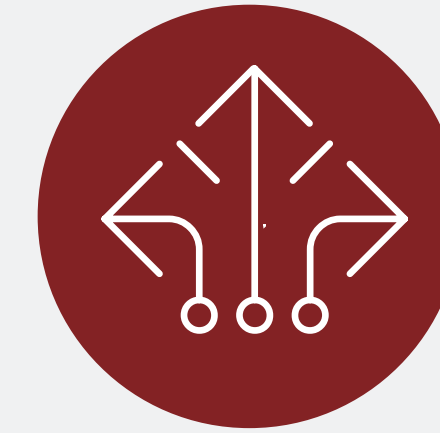
### 06 Operations security

Organizations should re-evaluate any configurations they made during the work from home period to ensure that they are still the most effective



### 07 Vulnerability management

Patching is a challenge even for an information resilient organization. In returning to the office, organizations must evaluate their patch posture, and where found wanting prioritization patching



### 08 Business continuity

It is now time to learn from recent activities – the remote working paradigm – and apply the acquired knowledge to improve the readiness of the business continuity plan



### 09 Incident management

Incident response represents the last line of defence should an attack materialize. Make sure your organization is set up in preparing for and responding to a data breach



### 10 Security governance

Risk Registers should be reassessed given the newly restructured threat landscape and control plane

#### Find out more

IE/International

Call: +353 1 210 1711

Email: [cyber.ie@bsigroup.com](mailto:cyber.ie@bsigroup.com)

Visit: [bsigroup.com/cyber-ie](https://bsigroup.com/cyber-ie)

UK

+44 345 222 1711

[cyber@bsigroup.com](mailto:cyber@bsigroup.com)

[bsigroup.com/cyber-uk](https://bsigroup.com/cyber-uk)

US

+1 800 862 4977

[cyber.us@bsigroup.com](mailto:cyber.us@bsigroup.com)

[bsigroup.com/cyber-us](https://bsigroup.com/cyber-us)

Italy

+39 026679092219

[cyber.italy@bsigroup.com](mailto:cyber.italy@bsigroup.com)

[bsigroup.com/cyber-it](https://bsigroup.com/cyber-it)