PRiSM INFOSEC

QUICK GUIDE

10 CHECKS FOR SECURING RAPIDLY DEPLOYED HOME WORKING

The essential guide for ensuring systems and data availability without compromising security

During these unprecedented times, organisations around the world are rapidly deploying home working for their employees. This can present a challenge in terms of maintaining functionality, performance and information security requirements. This 10 point guide provides IT Teams with a set of security considerations to ensure a strong balance is achieved between security and data and authorised systems availability.

1) MAINTAIN SECURE BUILDS

Build and deploy a secure machine image as quickly as possible and prioritise the most important security options for the organisation, such as full disk encryption, ensuring only user level access to the device, restricting access to removable media and enabling automatic updates.

2) HOME PC SECURITY

Discourage or ban access to company data from personal computers in employees homes. If this is not achievable ensure secure configurations are in place.

3) REMOTE ACCESS CONFIGURATION

Ensure that any rapidly stood up VPN / Remote Access technology is configured with strong authentication and encryption. Where possible, use an additional factor of authentication and the latest encryption technologies.

4) QUALITY OF SERVICE

Plan and implement user/client-based Quality of Service (QoS) limits on remote access endpoints. If not possible, implement QoS policies on client O/S to restrict network bandwidth.

5) CLOUD SERVICE CONFIGURATION

Review the configuration of cloud services, ensure they are optimal, restrict file sharing outside of the organisation and ensure log and audit settings are enabled.

6) CONTINUE TO ASSESS RISK

Implement a fast track risk assessment methodology that covers key information security controls and considerations the organisation needs to maintain, and ensure changes go through it and submit it to the management team.

7) MAINTAIN CHANGE CONTROL

Track all changes that are made either in an existing change management system, or use a simple spreadsheet or document template that tracks changes (e.g. date, time, resource responsible, systems affected, changes implemented, rollback procedure, reference to further documentation).

8) CYBER SECURITY AWARENESS

Ensure regular communication and updates with employees on the importance of information and physical security at home and risks of exposing company data over emails or unapproved resources.

9) PHYSICAL SECURITY AWARENESS

Ensure staff understand the risks of leaving devices unattended, especially in public places and how to report loss.

10) BE AWARE OF GUIDANCE

Be aware and use information security guidance from authorities such as the National Cyber Security Centre (NCSC), SANS Institute in the United States and reputable partners.

ABOUT PRISM INFOSEC

Prism Infosec is based in Cheltenham and Liverpool, UK and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations and has helped hundreds of companies to protect themselves from cyber-attacks. Prism Infosec is a CREST member company, a Cyber Essentials certifying body and is an 27001:2013 and ISO9001:2015 certified (UKAS-accredited) organisation.

☎ To book an assessment call:
+44 (0) 1242 652100

🌐 To buy online visit:
https://prisminfosec.com

✉ To send us an enquiry email:
contact@prisminfosec.com