smartdesc secure: Remote Working Toolkit

Cyber Security controls for charity remote working

How do you keep corporate data secure when nobody is in the office?

- Staff are using personal devices; How do you stop your corporate data being stored on personal devices unsecured?
- How can you keep company computers up to date and secure when they are all over the country?
- What happens if devices go missing with data on them?

The Smartdesc Secure Remote Working Toolkit contains 8 cyber security controls that have been developed through supporting hundreds of charity staff. It is a one-stop-shop to cover the biggest cyber security risks. It provides cost savings, and doesn't interfere with staff productivity.

- Reduce the risk to your charity from data loss caused by remote workers.
- Non-technical training to teach staff how to keep secure when working from home.
- Allow staff to use personal devices without risk of company data going missing.
- Centrally manage and maintain computers without a server, firewall or office space.
- Cyber Essentials Basic included.
- Smart Pricing – from £15 per seat per month.

Remote Working Policy

Built on the latest best practice, our IT and Governance Policy templates outline how staff should be working remotely. These are easily tailored to your organisation.

Microsoft 365 Secure Score

A bespoke report on the overall security of your charity's IT setup. To help close the gaps, the priorities focus on the highest risk areas such as two factor authentication and encryption.

Security Awareness Training

Bespoke, charity specific, interactive training delivered by the Smartdesc Security Team. Designed to focus on the biggest risks when working remotely: how to spot threats, and what to do if you encounter something suspicious.

Device Monitoring and Management

Devices being outside the office for so long mean they may be out of date, unpatched and invisible. Our Monitoring and Management solution allows devices to be maintained, managed, asset reported and even wiped if necessary.

Bring Your Own Device (BYOD)

Policies and controls to allow staff to use personal devices safely, without corporate data ending up on them by mistake.

Home Network

Home networks may be vulnerable if not setup correctly, however, they are now mission critical for most staff accessing corporate data. We provide simple to follow support and guidance to improve the stability and security of home internet connections.

Phishing Tests

Remote workers are especially susceptible to social engineering through malicious email. We run realistic but safe phishing emails that educate, inform and help staff ensure they do not to click on dangerous emails.

Cyber Essentials

Funders, Local Authorities and Grant Makers are increasingly asking for Cyber Essentials to be in place. We audit and award Cyber Essentials as part of the package.

Enquiries: 0203 440 2445
Support: 0203 440 2444

www.smartdesc.co.uk
@Smartdesc_ltd