smartdesc

smartdesc secure

Processes and Controls to Protect People and Systems

Anti-virus is not enough. As cyber-attacks become more sophisticated, both the GDPR and Information Commissioner have made it clear that appropriate technical and organisational security measures need to be in place. That means training, policies and processes as well as traditional security tools.

Individually, all these elements can add up to a considerable cost and administration overhead.

The Smartdesc Secure suite is a fully managed set of IT security services, available at a single fixed monthly cost – meaning budgets can be controlled and costs capped, without the need to juggle multiple systems and suppliers. It can provide efficiency savings of over £600 per month for a small to medium sized organisation.

This is more than a set of tools; it is an holistic approach to IT security, covering people, policy, governance and technical preventative measures. It also includes a proactive threat management service, to ensure your organisation stays ahead of emerging attacks.

▶ **Device and server protection and patching**

▶ **Bespoke Security Audit and Risk Register**

▶ **IT Security awareness training for all**

▶ **CyberEssentials readiness report**

▶ **Information Governance policies**

▶ **Proactive Threat Management**

▶ **Data Protection process flows**

▶ **Regular Penetration Tests**

Audit and Risk Register
A ground up gap analysis of security loopholes, output into a bespoke, prioritised Risk Register.

IT Security Training & Compliance
Awareness training for your staff, and compliance reports to see who has attended.

Compromised Accounts Check
Scans user accounts daily against a vast public database to check for exposure of credentials on the internet.

Threat Management
Smartdesc monitors the ever-evolving security landscape, informing and instructing on how to mitigate the risk from a new cyber attack.

AntiVirus & Patch Management
Actively monitors systems and files to prevent malware and viruses, and applies security patches to devices and servers. Checked daily by our Security Ops Centre (SOC).

Information Governance & Policies
Process flows and baseline documents to help your organisation align to best practice and legal requirements such as the Data Protection Act and GDPR.

Penetration Tests
Bi-annual tests internally and externally to spot vulnerabilities on your network.

CyberEssentials
Readiness assessment to help your organisation achieve certification

---