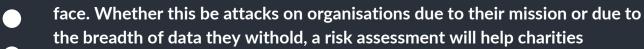# Making Charities Cyber-Secure

✓ Malware protection

Charities and their missions exist on a foundation of **trust** - they can prove their compliance and protect their reputation within the public eye by having malware protection in place to safeguard from harmful software and by training staff to only use trusted applications.

✓ Secure configuration

Secure configuration refers to security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities.

✓ Access control

Access control is the selective restriction of access to data within organisations and is put in place so that information does not fall into the wrong hands.

✓ Patch management

Patch management is about keeping software on computers and network devices up to date and capable of resisting low-level cyber attacks. This is one of the most important tactics charities can take to improve their cyber security.

✓ Boundary firewalls and internet gateways

A firewall is used for securing devices within a network and mitigating the risks of outsider attacks. Just one breach in an organisation can lead to damage to reputation and loss of trust, and for charities, perhaps a loss of donors.

CYBER ESSENTIALS

IASME GOV (includes Cyber Essentials)

Risk Assessment ✓

Risk assessments for individual charities will allow them to put in place procedures tailor-made for their size, purpose and specific threats they may face. Whether this be attacks on organisations due to their mission or due to the breadth of data they withold, a risk assessment will help charities understand their risk appetite.

Backup ✓

Ensuring that back-ups are consistently enforced across all data is crucial for charities so that they can safeguard against potentially catastrophic interruptions to the services they deliver, which needs to run smoothly so that help gets to those that need it fast.

Policies ✓

Ensuring that the right policies are in place across all aspects of a charitable organisation is imperative so that they have they know-how to combat security breaches as they occur.

Incident Management ✓

Incident management is put in place to ensure that the right handling of incidents reduces the impact of the incident on service users. With this in place, charities can prove to donors and other sections of their supply chain that they treat their data with the utmost care.

Data Protection ✓

To avoid facing costly fines, it is imperative that charities have data protection legislation is put in place across organisations.

Operational Management ✓

Putting procedures in place that ensure mistakes aren't made that could leave a system either set up or configured insecurely.

#cybersecurecharities