LPPA's cyber security measures

LPPA understands the importance of keeping member data secure. To ensure that the data under our control is kept secure, we have implemented a number of controls and technologies. Whilst technology is important in cyber security, the investment in training of staff is also a key factor in our defence against malicious acts.

LPP group (including LPPA) is ISO 27001 accredited and has Cyber Essential accreditation. This accreditation shows that it has processes and procedures in place that keep information and systems secure, which is independently verified.

System Security

All of LPPA's systems are protected at the network perimeter by firewalls, with Palo Alto firewalls in place at the main data centre. The firewalls are automatically updated to protect against emerging threats. Firewalls have a "default deny" policy, with changes to rules completed after a change control process is followed, with a business need and security review carried out. External penetration tests are carried out by CREST accredited organisations to verify the perimeter protection.

Servers and end-user devices are patched regularly, with critical patches installed within 14 days of release. All devices are covered by antivirus, which is centrally managed and updates are automatically downloaded to devices.

To protect against the loss of data, system corruption or ransomware, LPPA backs up data daily to tape, with tapes collected daily and sent to a secure, environmentally controlled storage facility. Data is restored regularly to test the restoration process and the backup media.

User Accounts & Access control

All users have dedicated user accounts, which require complex passwords. Domain accounts are protected with two factor authentication. Administrative accounts are separate from day-to-day accounts, with elevated privileges restricted to users who need them.

Access to systems and information is based on user role, with users only having access to data that they need, changes to user rights need to be appropriately requested. Access reviews are carried out regularly.

All default passwords and configuration is removed from new devices.

Incident Response

Whenever there is a risk to LPPA systems or data an incident response is started. The Security Working Group (SWG) is made aware and a response is handled by an Incident Response Team. The team is made up of representatives of the senior leadership team, risk, IT, communications and any other team affected.

Risk assessments are carried out whenever there is a critical vulnerability released, with both internal systems and suppliers monitored for their exposure and remediation.

External Services

Whenever an external software supplier is engaged, a risk assessment is completed, ensuring that the supplier has adequate levels of protection, security systems, encryption, processes and data is held within the UK where possible.

End Users and Home Working

With the move to home working, LPPA have had to implement changes to enable this. All users are provided with a company laptop, which is the only method they use to access systems. The laptops are protected with antivirus, web filtering, email filtering and archiving and are locked down to prevent unauthorised applications running. All company devices restrict the use of external devices to prevent homeworkers from connecting to personal printers etc.
All data on end user devices are encrypted using BitLocker, with users having to enter a code before the device boots.

Access to the LPPA network is via secure VPN using active directory credentials. The VPN client is updated regularly.

Improvements

Protection of data and systems is an ever-evolving area, with LPPA investing in improvements. LPPA is planning to implement a Security Operations Centre service in the next financial year, to improve its security profile.

The current DR process is being reviewed, moving to an online backup capability, whilst ensuring that backups will not be vulnerable to ransomware attacks.