Data Security Policy

Security is managed at a number of different levels within the application architecture & infrastructure - from user-level access to the application, down to the physical hardware running the application.

HTTPS Always On

Users accessing the Wicked Lab application are required to use the HTTPS protocol, ensuring that all web traffic between the users' browsers and the application server is encrypted and protected from 'man in the middle' attacks, or anyone attempting to intercept communication between users' browsers and the Wicked Lab application.

If a user attempts to use the insecure HTTP protocol (by visiting **http**://app.wickedlab.com) they will be immediately be redirected back to the secure site.

Role-based Accounts

All Transition Cards, Initiatives, Checklist and related data records are separated by account. Any user can only access data for accounts they are members of. That is, users may be members of one or more accounts, but only have access to data stored within those accounts and not any other.

Data Backup and Disaster Recovery

The entire system is backed up daily. In the advent of a complete system failure, the application can be rebuilt from scratch - utilising the most recent backup.

Application Security

We actively monitor Common Vulnerabilities and Exposures (CVE) publication lists, and routinely upgrade software in response to CVE announcements.

User passwords are not stored anywhere in the application. Instead we use the BCrypt hashing algorithm, an encryption protocol known for its resistance to brute force attacks.

Physical Security

The physical infrastructure is hosted and managed within a secure data centre. The hosting environment is certified to meet the IEC_27001 standard for information system security. This is considered the gold standard of system security, and requires the hosting provider to undergo regular audit to maintain compliance.

System Access

Remote operating-system level access to the Wicked Lab application is restricted to authorised personnel. Access requires two-factor authentication and all communication occurs over secure socket shell (SSH) connections. SSH connections are further protected using private/public keys.

While no system can be guaranteed to be 100% secure, we take great care in ensuring users' data is kept safe and secure. We regularly review our security processes - and those of third party suppliers - to ensure best-practise security procedures are maintained. And naturally we are always looking for new ways to further enhance the security of the system.