ABL Technology

Security Controls and Response Plan

ABL Technology Security Controls and Response Plan

Introduction

ABL Technology provides innovative, secure and reliable cloud based hosting and IT services to our clients around Australia. The ABL Technology was formed in response to a direct need for companies to deliver applications and information cost effectively and securely over the internet. Our team are experts in technologies well known and regarded in the industry, such as Microsoft Office 365 and Azure. We always follow vendor guided installation and security best practices, with all systems hosted with Microsoft Azure or on premise.

The ABL Technolgy team understand that security is a key consideration when adopting cloud-based solutions. This report outlines ABL Technology's approach to security and information privacy. It describes the organizational and technical controls used to protect client data and manage security related risk.

Security-first Culture

ABL Technology has created an active, “security-first” approach towards security and privacy. This company-wide culture ensures security is paramount and considered at all stages of the project to migrate your data to the cloud, and during the on-going support and maintenance of your systems.

Security Training

All ABL Technology employees undergo security training as part of the orientation and on-boarding process. New employees receive an induction program on ABL Technology commitment to keep customer information safe and secure. They also sign a non-disclosure agreement and user acceptance policy to ensure privacy of client data, protection of passwords, lockdown of administration accounts, and protecting client servers, data, devices and networks.

ABL Technology staff are regularly compliance tested to identify any weakness in security policies or staff requiring further training.

Data Privacy

On 22nd February 2018, new privacy laws were introduced for Australian businesses to notify the public when IT security breaches occur. Privacy Amendment (Notifiable Data Breaches) Act 2017. ABL Technology fully complies with the Notifiable Data Breaches scheme and has implemented an action plan if ABL Technology’s controlled infrastructure systems were ever breached.

At ABL Technology we understand the importance of ensuring the privacy of our client’s information and are committed to preventing unauthorized access or disclosure. We believe in prevention rather than a cure when it comes to protection of critical data. Client’s own all data they store or send and receive on cloud based storage. Data is backed up and retained for as long as they remain an ABL Technology client. If required, ABL Technology will provide an export of the client’s data at a minimal charge.

We regularly review our administrator access permissions to ensure only those people who require access have access, and that access is revoked when it is no longer required.

Operational Security

Security is an integral part of ABL Technology's operations. These activities include security risk assessments and compliance, active monitoring and reporting, logging and auditing, patch management, data protection, system policies and procedures, and Data Breach Response Plan.

Security Risk Assessments and Compliance

ABL Technology regularly undertakes security risk assessments on staff training, internal policies, security procedures and controls, and other critical security measures. The assessment includes identifying the key security risks, assessing the current security controls and providing recommendations for improvement. This approach ensures continual enhancement and allows ABL Technology to keep abreast of the latest security threats. ABL Technology also regularly undertake compliance tests on staff such as test email phishing campaigns, disaster recovery procedures, and simulated security events.

At the request of a client, ABL Technology often conducts similar security assessment reviews, security training and compliance tests on their client's users. To ensure a secure environment at every level, clients own internal procedures and policies must be reviewed to ensure their confidential data and systems are protected.

Monitoring and Reporting

All ABL Technology owned infrastructure systems are actively monitored for system performance issues, unauthorised security attempts, suspicious events and system outages. ABL Technology networks are protected at the perimeter by an advanced firewall which monitors and blocks known security threats from entering the network. The ABL Technology team regularly run security reports on where new threats are originating and if required, IP addresses or ports are added to our blacklisting.

At the request of a client, ABL Technology can provide a similar customised monitoring and reporting solution to their client's own internal networks.

Logging and Auditing

As per security best practices, the ABL Technology owned infrastructure enables event logging on all critical systems. Depending on system capabilities, settings are set to keep verbose history for 3 months, and show both authentication success and failures. This allows the ABL Technology team to investigate and trace system access throughout the entire infrastructure network.

Operational Security (continued)

Patch Management

ABL Technology follows a regular system maintenance procedure on all systems. This includes a fortnightly patch management program on ABL Technology own computers, servers and other critical systems. A monthly patch management program on core infrastructure systems including network and endpoint devices under ABL Technology's management. Any identified vender critical vulnerabilities are assessed and patched within 30 days.

Data Protection

ABL Technology's team is trained to ensure client data is protected at every stage. Copying of sensitive client data from protected client networks or servers to unsecured devices or networks is forbidden, without prior approval. Any data copied to removable media is cleaned and destroyed once the job is finished.

System Policies and Procedures

ABL Technology operates under the industry recognised ITIL (Information Technology Infrastructure Library) best practices for IT service management (ITSM). ITIL provides IT service providers with good-practice guidance on the design of the services, processes, and other aspects of the service management enterprise. ITIL covers the following main categories:

- Design coordination
- Service catalogue management
- Service-level management
- Availability management
- Capacity management
- IT service continuity management
- Security management
- Supplier management

Data Breach Response Plan

ABL Technology's incident management process involves a tried and tested practice to ensure security events are responded to within an agreed 2 hour timeframe. If a security event occurs, the event is logged in our ticketing system and the security response team is notified. The team encompasses 2 senior level technicians, and are trained in the Data Breach Response Plan.

The Data Breach Response Plan involves the following steps and required actions:

Suspected or known data breach

1. When an ABL Technology employee or contractor becomes aware or suspects that there has been a data breach, they will log a support ticket including all the details of the suspected breach and assign the ticket to the "Security Response Team" department within the ticketing system. They will also notify their IT Manager.
2. The IT Manager will then notify the IT Director and make sure the ticketing system includes the following details:

- brief description of the nature of the breach,
- how it occurred,
- the date of the breach,
- the date of discovery, and
- the date of notification to the IT Manager

3. The IT Director will also assign the user's manager, identified account contact, or data owner to the ticket as a CC. The IT Director will also contact the user's manager directly to confirm receipt of email.
4. Depending on the seriousness of the data breach, the IT Director will appoint a response team involving a staff member, or multiple staff members, or skilled external contractors to undertake the response process.

Contain

The response team will take immediate steps to contain the breach, which may involve:

- stopping the unauthorised practice;
- recovering records;
- shutting down system that have been breached;
- revoking or changing computer access privileges;
- addressing weaknesses in physical or electronic security; and
- alerting the appropriate authorities.

Data Breach Response Plan (continued)

Assess

1. The response team will determine the seriousness of the breach and determine whether the response time to contain the breach was adequate enough to contain (less than 24 hours), and/or the breach involved data which was deemed unlikely to result in serious harm. The ticket needs to be updated under the Security Breach Identification field with either of the following:

- Breach resolved within 24 hours (Not reported to OIAC)
- Minor Breach unlikely to result in serious harm (Not reported to OIAC)
- Major Breach likely to result in serious harm (Reported to OIAC)

2. If not reporting to OIAC, the ticket will be updated and closed. The user's manager, identified account contact, or data owner will be notified.
3. If reporting to OIAC, the response team will complete the Notifiable Data Breach Form via the OAIC websitehttps://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

Notification and Review

The response team will submit the Report to the Office of the Australian Information Commissioner and notify affected individuals or coordinate with the user's manager, identified account contact, or data owner. If the breach was identified as an internal ABL Technology breach, an internal review of the data breach by the response team will be conducted to ensure the threat is completely isolated and prevented from reoccurring.

Azure Infrastructure Security

Microsoft Azure Security

All client data and servers are hosted in a secure Microsoft Azure data centre located in East Australia. Your data is protected from theft, flood, fire, malicious damage, and power outages. Azure hosting can be summaries as follows:

- Build on a secure foundation - Protect your customers and organisation with multi-layered security across data centres, infrastructure and operations. With an investment of more than USD 1 billion in research and development and 3,500 security experts monitoring to safeguard your data, Azure is the cloud service that you can trust.
- Own your data - Be confident about where your data is stored. Azure's core privacy principle is that you own your data and it'll never use it for marketing or advertising.
- Work remotely, securely and productively - Empower your employees to work from anywhere, on any device, with cloud-based desktop and app virtualisation. Securely deploy and scale the only solution fully optimised for Windows and Office, to enable collaboration – in minutes.
- Build and scale without constraint - Gain unlimited scale for your applications with the only cloud platform that provides hyperscale relational databases and a fast NoSQL database with open APIs for any scale. Deliver resilient apps that adapt to your organisation's needs over time, supported by industry-leading Azure service level agreements.
- Run mission-critical systems with confidence - Azure provides enterprise-grade cloud infrastructure on which customers and partners can rely. This includes physical elements such as redundant power, networking and cooling, as well as software elements such as safe deployment processes, ineffective maintenance and failure prediction enabled by machine learning.

Data Security in Transit

The Azure AVD infrastructure uses the latest SSL in-transit encryption for all data sent between server and client endpoint. TLS 1.2 protocols, RSA 2048-bit SSL, SHA-256 ciphers ensure your data cannot be siphoned & decrypted.

Microsoft Azure Network Security

The Azure infrastructure network has been designed to separate client servers by virtual networks and multiple hardware and virtual based firewalls by default. Perimeter firewalls monitor and automatically block security threats in user sessions accessing the Internet. Core infrastructure and management networks are locked down to separate zones, and only authorised personnel can gain access.

Business Continuity

Our backup and Disaster Recovery (DR) procedures covers our Azure hosted servers and High Security Plans for the following critical events:

- human error;
- file corruptions;
- hardware failures;
- multiple server failures;
- storage area network failures;
- data centre failures;
- security breaches; and
- catastrophic events (subject to some increases in downtime).

ABL Technology maintains a structured and tiered backup and recovery policy to ensure data integrity, availability, and rapid restoration in the event of system failure, ransomware, or data corruption. Daily incremental backups are performed on all critical systems, with full backups retained as follows:

- Daily backups retained for 90 days
- Monthly backups retained for 6 months
- Annual (yearly) backups retained for 5 years

Email data is recoverable daily and retained for 7 years to meet legal and corporate governance requirements.

Essentials 8 Security Framework (Maturity Level 2)

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

ABL Technology' owned infrastructure includes foundational security controls aligned with Maturity Level 2 of the government's ACSC Essential Eight Security Framework.

Key measures include:

1. Application Control: Application whitelisting is implemented on key systems to prevent unauthorised software from executing, particularly on workstations and servers handling sensitive data.
2. Patch Management: Operating systems and third-party applications are patched regularly within a defined timeframe (within two weeks for security vulnerabilities), reducing exposure to known threats.
3. Macros: Microsoft Office macros are restricted to approved sources. Only digitally signed macros from trusted publishers can execute, unless authorised.
4. Application Hardening: Common applications (e.g. browsers, PDF readers) are configured to block or disable unnecessary features such as Flash, ads, and Java, limiting avenues for exploitation.
5. Restrict Admin Privileges: Admin rights are granted only based on role, with regular reviews and use of separate accounts for administrative tasks to prevent lateral movement in the event of compromise.
6. Multi-Factor Authentication (MFA): MFA is enforced for all remote access and privileged accounts, adding a second layer of defense against credential compromise.
7. Regular Backups: Data is backed up daily, with integrity testing and offline copies stored to ensure recovery in case of ransomware or data loss.
8. User Application Hardening: Common controls are deployed via Group Policy and endpoint management to enforce secure configurations across endpoints. In addition, end-to-end encryption is implemented to protect sensitive information, ensuring that data remains secure both in transit and at rest.

These practices establish a resilient baseline against targeted attacks while demonstrating structured, risk-based control implementation across systems and users.

At the request of a client, ABL Technology can provide an essentials 8 security solution to their client's own internal networks. Available under our High Security Managed Service Plan.

ABL Technology - IT Support Plans

MSP Support - Managed Service Provider Support (Business L1)

- Unlimited Remote Support (12x5: 8am - 8pm Mon - Fri)
- Guaranteed 2 Hour Response on critical desktop support events within business hours
- O365 and PC/Laptop Device Support
- Quarterly performance / health reporting
- Desktop Advanced Security Software Package - Cloud based Malware / Virus Protection / Proactive threat insights
- Online Cyber Security Onboarding and data breach response logging
- Office 365 email and data backup / recovery
- Device monitoring software and alerting to ensure problems are resolved quickly
- Centralised Email Signature Platform

*Please note that this plan includes basic business PC security, if you store sensitive customer information you should be implementing the extra security controls which are included in the Corporate and High Security Plans.

MSP Support - Managed Service Provider Support (Corporate L1/L2)

- Unlimited Remote Support (12x5: 8am - 8pm Mon - Fri)
- Guaranteed 2 Hour Response on critical desktop support events within business hours
- O365 and PC/Laptop/Network/Server Device Support
- Monthly performance / health reporting
- Desktop Advanced Security Software Package - Cloud based Malware / Virus Protection / Proactive threat insights
- Online Cyber Security Onboarding and data breach response logging
- Office 365 email and data backup / recovery
- Device monitoring software and alerting to ensure problems are resolved quickly
- Centralised Email Signature Platform
- Regular Cyber Security email testing
- IT strategy and review sessions, as required
- Azure Active Directory device enrolment and basic conditional access policies (All devices must be running Win Pro and O365 Business Premium. BYOD is not recommended)

MSP Support - Managed Service Provider Support (Corporate High Security)

- Unlimited Remote Support (12x5: 8am - 8pm Mon - Fri)
- Guaranteed 2 Hour Response on critical desktop support events within business hours
- O365 and PC/Laptop/Network/Server Device Support
- Monthly performance / health reporting
- Desktop Advanced Security Software Package - Cloud based Malware / Virus Protection / Proactive threat insights
- Online Cyber Security Onboarding and data breach response logging
- Office 365 email and data backup / recovery
- Device monitoring software and alerting to ensure problems are resolved quickly
- Centralised Email Signature Platform
- Regular Cyber Security email testing
- IT strategy and review sessions, as required
- Azure Active Directory device enrolment and basic conditional access policies (All devices must be running Win Pro and O365 Business Premium. BYOD is not recommended)
- Threat Locker Application Whitelisting
- Essentials Eight ASCS Security Standards (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained)