Boardingware

Information Security Management

TECHNICAL WHITEPAPER

LAST UPDATED: May 1, 2018 10:34 AM

Contents

Introduction

Purpose of this whitepaper

Boardingware provides a secure cloud based platform to help schools improve student safety, increase operational efficiency, and protect student records. As a processor of student information, we understand our customers strict data protection obligations and have adopted industry best practices to ensure that we can protect the confidentiality, integrity, and availability of the information entrusted to us. This document summarises our processes, policies and security standards we employ, to help you understand our data security practices.

Executive Statement

At Boardingware, we take our responsibility to protect your data very seriously and pride ourselves on being a trusted partner to all of our schools. To ensure that we meet the expectations of our customers, we have embedded information security into the heart of our company culture. Our executive team have taken on leadership roles to manage the implementation, maintenance and communication processes, and are fully committed to ensuring information security is practiced in all aspects of our organisation.

Supporting Documents

In addition to this document, we have created the following whitepapers to further describe our security practices in more detail.

- Cloud Security Whitepaper - An overview of our security practices specifically related to cloud systems.
- Privacy Policy - Our policy to protect the personally identifiable information of our customers and end-users.
- GDPR Whitepaper - A brief demonstration of how we comply with the new General Data Protection Regulations.

Compliance Programmes

To provide security assurance for our customers, Boardingware has met compliance for several internationally recognised information security standards. The following section describes the international standards that we follow:

ISO/IEC 27001, 27017, 27018

Boardingware is currently in the process of achieving certification for ISO/IEC 27001 in alignment with ISO/IEC 27017 & ISO/IEC 27018.

Why ISO

The International Organization of Standards provide globally recognised specifications for products, systems and services to ensure quality, safety and efficiency. ISO has a network of over 160 national standards bodies each representing individual countries and have published over 22,000 international standards in 70 years. ISO standards take into account the needs from all their member countries to design specifications that are internationally recognised. Categories of ISO standards are compatible with a range of specialised supplementary standards, allowing Boardingware to double-down on specific areas of information security and provide a platform to build off in the future.

Boardingware is an international company serving schools in over 13 countries and ISO provided the most holistic international framework that took the needs of these customers into account. In addition, many other leading technology companies have gained certification in ISO 27001 as a recognised and robust framework for information security practices within the IT and Cloud industry.

Furthermore, our customers often hold information belonging to students and parents from all over the world. By aligning with ISO standards we have helped our customers meet the information requirements of their own countries as well as the countries of international parties.

ISO/IEC 27001

This standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation.

ISO/IEC is a certifiable standard which assures customers that certified companies have met the requirements of the standard.

ISO/IEC 27017 & 27018

In addition to ISO 27001, Boardingware has aligned with supplementary standards which focus on specific areas that are important due to the nature of our service.

ISO 27018 focuses on the protection of personally identifiable information (PII) as a PII processor. This standard provides additional controls which help Boardingware to...

- Comply with applicable obligations when acting as a PII processor
- Promote transparency in relevant matters to customers
- Facilitate appropriate agreements between customers
- Provide customers with a mechanism for exercising compliance rights and responsibilities

ISO 27017 provides additional information security controls to those outlined in 27001 which are intended to mitigate the risks that are associated with the technical and operational features of a cloud customer and provider.

Certified By The British Standards Institute (BSI)

The British Standards Institution is the first national standards body in the world. It was originally founded in 1901 and has since served as the internationally recognised standard for information security. The BSI primarily administrates a number of important international management systems assessments and certifications, including the ISO standards that Boardingware has chosen to comply with. Boardingware is scheduled to be certified by the BSI later this year.

GDPR

In the process of achieving ISO certification, we have also adapted our information management processes to comply with the new General Data Protection Regulation (GDPR). For more information, please refer to our Whitepaper: Navigating GDPR Compliance.

Boardingware's Information Security Management

To comply with the standards mentioned in the previous section, Boardingware has carefully implemented several processes and policies in all aspects of our organisation. The following section provides a brief overview of these security processes:

Business Continuity Management

Boardingware has established a business continuity policy to ensure that the management team allocate the proper leadership and resources so that the company is well equipped to respond to any potential risks that could disrupt or affect the delivery of Boardingware products and services to customers.

Disaster Response Plan

A disaster response plan has been put in place to prepare Boardingware employees to recover critical assets and services in the case of a disaster event. The plan defines a Recovery Time Objective (RTO) and a Maximum Acceptable Outage (MAO) for critical business activities and services. Detailed steps have been outlined to recover critical IT infrastructure. This plan is regularly rehearsed and revised to ensure it is up to date and effective in a disaster event.

Communication

Responsibilities and targets have been defined for alerting customers of any events that may have an adverse effect on the integrity, availability and confidentiality of their information. Providing customer support and communication is classified as a highly critical activity during a disaster event.

Incident Management

Boardingware has established guides to ensure that there is a consistent and effective approach to the management of information security incidents, including the responsibility of reporting security events and weaknesses.

All employees are responsible for reporting security events and are trained to follow the correct internal reporting procedures. Mechanisms have also been established for external parties to report security events through public channels.

Assessment & Response

Procedures for assessing and responding to incidents have been established to effectively manage the resolution and communication for different types of events.

Subsequent Actions

Processes for reflecting and learning from security incidents have been defined to isolate failures in Boardingware's information security system and to take corrective actions to reduce the frequency and impact of similar occurrences in the future. When applicable, disciplinary actions are carried out if employees commit a security breach which results in a security incident.

Human Resources

Multiple controls have been implemented to ensure employees and contractors uphold Boardingware's information security requirements throughout the entire employment lifecycle.

Screening

Background screening is carried out in accordance with relevant laws and regulations for all employment and supplier candidates during the recruitment phase.

Training and Awareness

Training programmes have been implemented during employee induction to ensure employees are aware and capable of performing their information security obligations. Sessions are held for introducing employees to applicable policies and procedures and updates are communicated for any changes to policies.

Employee Agreements

All employees sign a statement of acceptance confirming that they understand and promise to uphold the rules of Boardingware's information security management system. Information security responsibilities are also defined within employee and contractor agreements.

Disciplinary Processes

To ensure Boardingware's security controls are honoured, all employees are subject to disciplinary actions if they breach information security rules. Disciplinary procedures are outlined to consider the severity of the breach and the appropriate disciplinary actions. In severe cases, employees may be terminated.

Employee Termination

When an employee leaves Boardingware, they must return all information assets they have and all their access rights to information assets are revoked. Procedures exist to ensure this process is carried out in a timely and effective manner. Before departure, employees must sign a declaration which confirms they have rescinded access to all Boardingware assets and will continue to uphold Boardingware's information security rules after their employment has ended.

Secure Development Principles

Guiding principles have been established to ensure that information security is taken into account throughout the entire development lifecycle. This promotes a secure by design culture within Boardingware resulting in software products and systems with a high level of security. These principles apply to all types of development within Boardingware, including the creation of marketing systems, customer support systems, internal operations systems, as well as the development of cloud web and mobile applications.

Planning and Analysis

Security analysis is conducted during the inception of any new development projects. This analysis includes considering the impact of changes to the existing system, technical requirements, security requirements, and the identified risks. Results are documented and project leaders must ensure requirements are fulfilled throughout development.

Design and Implementation

Design and implementation guides are outlined to promote a methodical approach to developing projects effectively and securely. This includes development methodologies, version control, quality assurance, secure development environments, restrictions to

software packages and rules for outsourcing development.

Testing and Deployment

Strict guides for testing have been outlined to ensure secure and robust project outcomes. This includes testing requirements for different types of development, testing methods, rules for test data and reviewing changes to existing systems.

Deployment procedures are designed to release new features within little to no disruption to existing services and to ensure rollback capabilities are available in the case that a deployment goes unexpectedly wrong.

Monitoring and Maintenance

Considerations for monitoring the effectiveness of projects throughout all the development phases are taken into account. Important metrics are decided upon during planning and implementation then tracked after deployment.

Continued maintenance of new projects are taken into account including the consideration of future updates and ongoing overheads to ensure the continued quality and reliability of releases.

Information Classification

Rules are defined to ensure appropriate classification and protection of all the information Boardingware handles.

Information classification is determined by the value, sensitivity as well and contractual obligations associated with information types. Classifications are organised by confidentiality which dictate access control and information handling rules. Classified information is clearly labelled to ensure proper treatment.

Acceptable Use Of Assets

Boardingware has defined clear rules for the appropriate use and responsibilities of information assets.

Software Installation

Restrictions are placed to control software installation on organization assets. Only software which has been approved after a risk assessment may be installed and any software that breaches copyright laws or has been developed by untrustworthy developers are prohibited. Requests for installing new software must follow detailed procedures.

Configuration Of Employee Computers

All employees are provided MacBook work computers which are configured to ensure information is protected from unauthorised access and accidental loss. This includes enabling hard drive encryption, firewalls, password requirements and malware protection.

Backup

All company information must be backed up and stored online within the appropriate company approved and managed cloud services and not stored exclusively on local machines. Additional backup requirements are specified for highly critical information.

Clear Desk and Clear Screen

Sensitive classified information must be removed from desks, screens and shared areas when unattended to prevent unauthorized access. Work computers must be password locked when unattended.

Internet Usage

A secure private network is provided for employees separate from guests. All work related activities must use the company's secure network unless when working in accordance with the teleworking policy. The company network is managed with enterprise grade appliances and software. Access to web pages can be controlled and employees are not allowed to bypass such restrictions.

Electronic Messaging

Only approved company applications may be used to communicate work related activities and transmit company information. Highly sensitive information types are restricted to specific channels and require additional encryption controls.

Intellectual Property Rights

Employees are not authorized to make copies of company information unless when permitted by law and when doing so within the guides of Boardingware's information security rules. Making copies of software of other original materials which infringe on copyright laws is prohibited.

Company Devices

The following controls have been laid out to effectively manage the use and configuration of company devices:

General Use - Use of company computers is limited to work purposes or legal personal activities which do not infringe on Boardingware's information security rules. An acceptable use policy has been established to clearly defined these guidelines.

BYOD - All work computers used by employees are owned and managed by Boardingware. Computers or devices which are not owned by the company are not permitted to be used for work purposes except for a few exceptions. Personal mobile devices may be used for limited work purposes in accordance to the Mobile Equipment Policy and in some cases where a lot of sensitive information is being handled, a company phone is provided. Computers that are owned by contracted developers must be configured and managed in accordance to Boardingware's Supplier Security Policy.

Mobile Equipment - When using mobile devices, employees must take special care to avoid unauthorised access. Devices may not be left unattended in an insecure manner which is outlined in a Clear Screen Policy. Rules outlined in the Information Classification Policy are applied to protect classified sensitive information. Devices are only permitted to connect to trusted WPA2 password protected networks. These guides direct employees to take special care to protect against unauthorised access of information if they are working in public areas such as airports or cafes which is generally discouraged unless unavoidable.

Device Manager - Boardingware has implemented enterprise grade mobile device management software which allows the CISO to remotely control, configure and monitor the use of company devices. Once the MDM is installed on a device, the proper configuration settings are enforced and cannot be overridden by the user ensuring security controls are consistent and effective across the organisation. Any misconfiguration or misuse of a device can be tracked and mitigated from a centralised dashboard.

Teleworking

Boardingware serves customers from around the world which requires various staff members to work from different countries. In addition to all other information security rules, special controls are stipulated for employees or contractors who are considered permanently teleworking outside of the head office. This includes restrictions on the use of work computers, mobile storage devices, and additional rules to leaving company devices unattended. The CTO must also assess and confirm the security of their primary network meets the security requirements.

Taking Assets Off-site

Controls are implemented to ensure appropriate protection and responsibilities are established when taking assets off site, including keeping records of each event.

Secure Disposal Of Media

Guides have been created to ensure employees securely dispose of sensitive information and equipment including the destruction of mobile storage devices, paper documents and cloud computing environments.

Access Control

Policies and systems have been implemented to assign appropriate access controls to company assets based on Boardingware's business and security requirements. These controls are intended to enforce that access to information is managed on a "need to know basis", employees protect their access and information is accessed securely.

Access Management

Access profiles are defined by business functions and determine which assets an employee is allowed access to by default. This is limited to a 'need to know' and 'need to use' basis and request processes must be followed to gain special access to assets that are not assigned to a role. Specific controls are assigned for privileged access rights such as administrators of applications. Asset responsibilities are defined and asset owners for each asset are assigned. Guides for accessing networks ensure WPA2 and SSL protection is enabled when transmitting sensitive information. The most sensitive information is only available through authorised IP addresses.

User Management

Boardingware personnel are assigned unique IDs which must be used for registering to business assets. Each account uses this ID which enables Boardingware to track use of assets and hold employees responsible for their correct use. Access can be revoked upon termination or in the event of compromised user accounts. The CISO and asset owners are responsible for regularly reviewing and altering access rights to ensure correct access is assigned to all assets.

Password Policy

A password policy is in place to ensure employees set strong passwords and manage their protection effectively to protect against generative password attacks. Rules for sharing and inputting passwords are enforced to avoid unauthorised disclosure.

Password Manager

An enterprise grade password manager is implemented to ensure all employees have effectively managed their access credentials. Multi-factor authentication and highly secure passwords is mandated for the use of the password manager.

Support and Escalation

Escalation Process

In addition to incident response procedures, Boardingware support personnel are provided escalation procedures to internally raise the priority of support issues that may have an adverse effect on the integrity, availability and confidentiality of customer or end user information.

Accessing Customer Accounts

When Boardingware personnel access customer or user accounts, explicit permission from the account holder must be recorded. Only actions which fulfill the purpose for which access was granted are allowed and employees must log out immediately after completing the necessary tasks. Access to customer accounts are restricted to approved employees and networks only. All actions conducted by Boardingware personnel within customer or user accounts is auditable and can be traced back to user IDs, timestamps and CRUD (create, read, update, delete) details.

Cryptographic Controls

Cryptographic controls are used throughout Boardingware's operational systems and products to ensure protection of critical business information and compliance with any legal, regulatory or contractual obligations. This includes the encryption of confidential or sensitive information, encryption of networks, encryption of work devices, and detailed encryption specifications to be implemented throughout the development of Boardingware's cloud and mobile products, such as - encryption at rest and in transit.

Supplier Security

Supplier security policies have been established to ensure the correct management of supplier relations throughout the supplier lifecycle. Suppliers include development contractors, Cloud software as a service providers (SaaS), infrastructure as a service providers (IaaS), financial, accounting and legal consultants.

Screening

Background checks and reference checks are conducted to assess the legitimacy and track record of prospective suppliers.

Access Control

Pre-defined access controls determine what information types each supplier type is authorized to access as well as procedures to restore unapproved access to information.

Requirements

Before access to information is granted the suppliers must meet the predefined minimum requirements to access information types they require. For example, to gain access to customer and end user PII, suppliers must ensure Boardingware can meet it's data privacy legal and regulatory obligations.

Agreements

Supplier agreements are in place to ensure that suppliers are obligated to meet the minimum requirements of the supplier security policy, ensure that Boardingware meets it's legal and regulatory obligations, service and security levels are maintained or exceeded, secure transfer of information, confidentiality of information and return of information at the expiration or termination of contracts.

Training & Awareness

When necessary Boardingware will provide training and awareness to suppliers to ensure they are aware of the rules stipulated within the supplier security policy.

Monitoring and Review

Contract owner responsibilities are assigned to Boardingware personnel to ensure the continued maintenance and review of supplier services in accordance to their adherence of agreements and quality of services provided.

Conclusion

We take security seriously at Boardingware, because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust.

Boardingware