Contents

Thinking Cap Risk Management Program

Our Risk Management is broken into 3 main parts. These are information security, information integrity and system availability. The first area is around securing data from unauthorized access. We review data access policies and practice, data transmission standards and security of data at rest. Integrity risks are around loss of data by mistake or environmental failures and how we keep these factors from leading to data loss. Finally, the last risk is around continuous availability of the LMS service. This last one looks at the redundant services we use to ensure we can deliver on our service SLA.

Information Security

We have a written information security policy, approved by management, published and communicated to all employees, contractors and relevant external parties in a way that requires employees to certify their understanding and compliance before access is granted and at least annually.

The group of people on staff with this access to customer data have been with the company for over 7 years. All gained this access after years of demonstration of this understanding. Key policies for Physical Security include:

- We have documented and assigned security responsibilities.
- There is a formal process in place to screen employees and contractors including a criminal background check on all staff that have any access to customer data.
- Access is reviewed for all employees at least every 6 months.
- Shared user accounts are prohibited.
- When an employee leaves the company, employee's user accounts and passwords immediately revoked.
- We maintain an inventory of all Hardware and Software IT assets.
- We have a formal IT asset decommissioning process in place including secure destruction of all electronic media. This includes hardware asset destruction with prior secure wipe.
- We have a formal process in place to ensure all sensitive paper-based information is adequately controlled and destroyed when no longer needed. We have a clean desk policy for controlling sensitive paper-based information and have a shredding process in place to destroy sensitive paper-based information.
- Client data is completely walled off from other clients. It is stored only in data centers with PCI Level 1/ SOC 1/SSAE 16/ISAE 3402 and SOC 2 Compliance verified by 3rd Parties. All data is stored encrypted at rest.
- All Hardware used to deliver the Thinking Cap service is within and managed by Azure and AWS data Centers.

Physical Security

We secure physical access to offices where Client data will be stored/accessed using an electronic access control system.
We maintain physical access surveillance and logging capabilities for your offices including;

- Visitors to offices are required to sign in and records are retained for at least 3 months.
- Entries and exits to building are under monitored and recorded video surveillance.
- Entries and exits to Thinking Cap office are under recorded video surveillance.

- No member of Thinking Cap has physical access to any data center. All access to data centres are managed by Azure and AWS.

Network Security

Developers and Support Team have ongoing access to perform changes in the production environments, but all changes made by them are logged and all data is time stamped.

Network security technologies controls that are implemented in the Thinking Cap environment.

- Boundary is protected with a firewall with ingress and egress filtering.
- Public facing servers are in a well-defined De-Militarized Zone (DMZ).
- Internal network segmentation is used to further isolate sensitive production resources.
- Wide area networks, including MPLS are private fiber or encrypted.
- Network Intrusion Detection or Prevention system are on the network and actively monitored.
- Host-based Intrusion Detection or Prevention system are on hosts and actively monitored.
- All remote access requires 2 factor authentications e.g., RSA tokens.
- All desktops are protected using regularly updated anti-virus software.
- Servers are protected using regularly updated anti-virus software or OS appropriate countermeasures against viruses.
- Servers are protected using relevant hardening practices.
- The network and hosts are regularly scanned for unauthorized or vulnerable configurations. e.g., port scanning, vulnerability scans.
- All OS, network devices and applications have vendor supported patches available and are actively kept up to date with available patches.
- All wireless networks are isolated from the corporate network or secured with WPA2.

Application Security

Thinking Cap Application maintains minimum Application security standards including but not limited to:

- Federated identity / single sign-on (SSO) available for all System access
- Password Management in the Application
- Password strength requirements.
- Passwords are changed on a periodic basis.
- Password reuse restrictions are enforced.
- Account lockout after predefined invalid attempts, after which intervention is required to unlock the account.
- Initial passwords must be changed immediately after logon.
- Passwords must have a minimum length of 8 characters.
- Passwords must include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, non-alphanumeric symbols.
- Passwords must be changed every 90 days.
- Passwords stored Encrypted and Salted.
- Must not match previous passwords and password reuse restrictions are enforced.
- Must never be transmitted in unencrypted form.
- Must never be stored in unencrypted or unsecured form.
- Account lockout after ten (10) consecutive invalid password attempts, after which intervention is required to unlock the account.

Data Transport and Storage guidelines include but are not limited to:

- Data is encrypted in transit on external public networks, including the Internet with a minimum of TLS 1.2
- Data is encrypted in transit on internal networks.
- Data is encrypted using at least WPA2 on wireless networks.

- Data is encrypted in storage on servers, e.g. databases and fileservers.
- Database Encrypted at Rest.
- Data is encrypted on backup media.

Information Integrity

We have a backup procedure in place for all Client data including Database and Storage. We can restore some or all data back a minimum of 30 days.

All Logs are kept by the Thinking Cap application are maintained for as long as a client is a Thinking Cap customer and 6 months after.

Security event and log data is regularly reviewed on an ongoing basis in the course of performing our duties. We log every action taken by any user or via the system. We also make these logs available to our customers who can perform any analysis they wish. Also, the vast majority of access to our system is done via SSO and those client SSO systems are responsible for application Access Management.

Changes and approvals to System Functionality are tracked and auditable via internal ticketing system.

Patch management is done through centralized patch management servers for ALL Operating Systems.
Our software development process for security review and approval prior to release includes the following steps:

- Architecture or Design Review.
- Threat Modelling.
- Manual Implementation or Code Review.
- Functional Verification and Testing.
- Penetration Testing.
- 3rd Party Software to find commonly known security holes in code is run at each release against our Code Repository.

We maintain a developer security training curriculum that must be completed by our product developers.
We provide a copy of a recent manual or automated penetration test report for your developed product with each major release.

All medium to Crucial findings are reported to senior management. We resolve or mediate all Crucial, High and Medium findings ahead of release.

With each Release or Patch we provide detailed Notes indicating all changes to the Application and results of our Automated and Manual Functional Testing.

An Information Security Incident Management plan exists including policy to provide formal documentation to clients and other responsible parties.

System Availability

The underlying System Architecture of Thinking Cap is based on redundancies for all system resources. Both Azure and AWS hosts provide redundant storage and computational resources in data centers no less than 500 miles away from each other.

Thinking Cap maintains a Service Level Agreement with all clients for 99.9% System uptime. Additional Guarantees for Application support are as follows.

Initial response times are within 2 Hours working hours for any non-critical ticket. Thinking Cap support hours are typically between 8am and 6pm (Eastern Standard Time; GMT -5), Monday to Friday, except to resolve crucial Issues. Public holidays are as per those for Ontario, Canada.

Resolution times are dependent on the priority levels of the issues involved and are subject to the cooperation of the Client in providing the information required when logging technical issues in Issue Manager and responding to Thinking Cap's questions in Issue Manager within 24 hours (working week).
Issues will be raised according to the following priority levels:

Priority 5: Server Down

The Service is "down", operation of the Service is severely degraded, or there is a crucial impact to the Service due to a fault with the network or other software issue. There are no workarounds. Examples include total loss of service (unscheduled downtime) and significant security breaches; admins cannot work in any domain or receive 5xx error messages.
•Server Down issues must be ticketed on Issue Manager as soon as the Client becomes aware of them on a 24/7 basis, however it is assumed that Thinking Cap will already be aware of any true 'server down' issues thanks to external server monitoring tools.

•Thinking Cap will respond to Server Down issues immediately. Given the major impact of a crucial issue, Thinking Cap will seek to implement a fix within 24 hours and will do so without first seeking approval from the Client.

•Thinking Cap will provide Client a named representative, at the appropriate senior technical level, with an emergency 24 hour mobile phone number to support the mitigation of issues of a crucial nature.

Priority 4: Crucial

The operation of the System is compromised or causing specific issues which are negatively affected by inadequate performance of the network or other software issues.
There may be partial or no workarounds, but the overall operation of the System is affected to the extent that the Client's customers, staff and other stakeholders cannot use the system for the purpose for which it was originally intended.

•An example of such an issue for LMS Admins would be when part of the System (e.g. one domain) is inaccessible or tasks cannot be carried out (e.g. creating new domains), thereby delaying our ability to modify or create existing or new domains.

•An example of such an issue for a learner would be when part of the System is inaccessible - for example, they cannot load their e-learning course(s), submit or review marked assignments, or access a forum for a moderated course.

•Thinking Cap will provide resources during their normal business hours to resolve the situation and additional resources outside of normal business hours as reasonably necessary. Thinking Cap will resolve the issue and update Issue Manager with details within 24 hours or sooner, with the expectation that said issues will be resolved within 48 hours of initial report or as mutually agreed (e.g. holding for a patch or release date).

Priority 3: Major

The System is functioning but has issues which affect a feature or a set of features – it impedes or inconveniences but does not prevent users from continuing their course. For example part of the System is not functioning as per specification but it is not business-critical issue and does not affect the ability of learners to access their learning materials on the LMS.

•Thinking Cap will resolve the issue and update the ticket within 3 working days of initial report or as mutually agreed (e.g. holding for a patch or release date).

Priority 2: Normal

The System is functioning, but there is a cosmetic or user interface issue and the customer is not prevented, not impeded or inconvenienced. Operational performance of the Service is not impaired. For example an issue that affects the appearance of the system but not its functionality.

•Thinking Cap will resolve the issue and update the ticket within 15 working days of initial report, or as mutually agreed (e.g. holding for a patch or release date).

Priority 1: Minor

The System is functioning, but there is a user interface issue that could be improved and there is no reported inconvenience to customers, or a Change Request is being submitted for discussion. For example, the Client requires information or assistance with Service's capabilities, installation or configuration and there is little to no effect on its business operations. Included are requests for information, assistance, features, alpha/beta and others.

•Such requests will be responded to within 48 hours. Issues will be either escalated for resolution within the agreed time frames, closed, or may be designated as 'Postponed' for as long as is deemed appropriate.

Privacy Policy

Thinking Cap is committed to maintain client privacy and to provide the tools needed to allow our clients to maintain privacy for their clients and users. We serve clients with many different Privacy requirements including FDA CFR 21 Part 11, HIPPA and GDPR.

Our primary Privacy standard that dictates our internal policy and procedures is the General Data Protection Regulation (EU) 2016/679 (GDPR). To this end we commit to:
Process the Personal Data only to the extent, and in such manner, as is necessary for the purpose of carry out its duties in accordance with the Client's written instructions and this clause (unless otherwise required by European Union laws or the laws of the European jurisdiction in which we Processes the Personal Data; or unless otherwise required by laws outside the European Union.

Implement appropriate technical and organizational measures in accordance with the Data Protection Legislation to ensure a level of security appropriate to the risks that are presented by such Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the likelihood and severity of risk in relation to the rights and freedoms of the Data Subjects;

Ensure it has taken all reasonable steps to ensure the reliability and integrity of any employees or other persons authorized to process the Personal Data.
Assist and co-operate with the Client as requested to ensure the Client's compliance with its obligations under the Data Protection Legislation.

Notify the Client promptly (and in any event within 24 hours) of becoming aware of any actual, suspected or threatened Personal Data Breach of any component of the Personal Data;

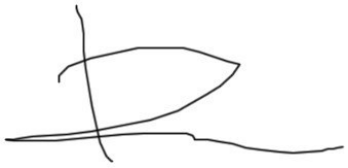
Ensure that such notice includes details of the nature of the breach, including the categories and approximate number of Data Subjects and records concerned and the remediation measures being taken to mitigate and contain the breach;

Provide prompt assistance as requested by the Client following the notification of an actual, suspected or threatened Personal Data Breach.

The Thinking Cap Application provides functions to Anonymize User data both via Automated and Manual systems to “forget” defined portions of a User’s personally identifying data where accounts is unused or terminated or where such action is requested by an individual.

Approval

Per:



I have the authority to bind the company.

Name: Douglas Wallace
Title: President
Date: January 26th, 2022