Security & Privacy

Useful Information for Privacy Impact Assessments & Threat Risk Assessments

PEASI

p: (888) 400-5661
e: info@peasi.com

Table of Contents

Introduction

As our company continues to evolve and expand, protecting our assets, sensitive data, and the confidentiality, integrity, and availability of our systems is paramount. We recognize the ever-increasing nature of cyber threats and the potential impact that security breaches can have on our operations, reputation, and customers.

Our security architecture covers these three main areas, with each area having unique challenges and requirements. Application security aims to protect our systems and data by securing our software applications, implementing secure coding practices, conducting regular vulnerability assessments, and ensuring that employees are trained and aware of potential risks.

Data security aims to protect our sensitive data against unauthorized access, theft, or loss through measures such as data encryption, access controls, regular data backups and disaster recovery procedures.

Finally, network security is essential to ensuring the integrity of our systems and preventing unauthorized access or data breaches through the implementation of firewalls, intrusion detection and prevention systems, and regular security audits.

Application Security

The security of an application is crucial in today's digital world, as cyber threats continue to evolve and become more sophisticated. To ensure the confidentiality, integrity, and availability of data, it is essential to implement a set of robust application security principles and measures.

By following established application security principles and implementing a set of security measures, organizations can protect against potential threats such as unauthorized access, data breaches, and cyberattacks, ensuring the confidentiality, integrity, and availability of their applications.

Application Security Principles

We understand the importance of protecting our applications from potential security threats. These principles serve as the fundamental guidelines for designing, developing, and maintaining secure applications. By implementing these principles, we aim to ensure the confidentiality, integrity, and availability of our applications while mitigating the risks of potential security incidents. It is our responsibility to follow these principles to establish a strong

foundation for our application security strategy and provide our customers with the highest level of security possible.

- Secure by Design: Security is essential to the application's design and development process.
- Principle of Least Privilege: Access to application resources is restricted to only authorized personnel on a need-to-know basis.
- Defence in Depth: Application security measures are implemented at multiple layers, such as network, application, and data levels, to provide overlapping protection.
- Secure Configuration: The application is configured securely to minimize potential security risks and vulnerabilities.
- Secure Coding Practices: Secure coding practices are followed to minimize potential vulnerabilities and ensure that the application is resistant to attacks.
- Regular Security Testing: Regular security testing is conducted to identify potential security risks and vulnerabilities in the application.

By following these principles, organizations can design and implement an effective application security architecture that protects against potential security threats, ensures compliance with regulations, and provides a foundation for continuous improvement.

Application Security Measures

We follow a set of application security measures to ensure the security and integrity of our applications. These measures help us to detect and prevent potential security incidents, ensuring that our applications are safe and secure for our users. By implementing these measures, we can minimize the risks of unauthorized access, attacks, and vulnerabilities, and maintain the confidentiality and privacy of our users' data. Our commitment to application security is essential in building trust with our users and ensuring the success of our business.

Input Validation: Validate and sanitize all inputs from users to prevent SQL injection, cross-site scripting (XSS), and other injection attacks.

Authentication and Authorization: Ensure that users are authenticated before they can access the application, and that access to resources is authorized based on the user's role and privileges. Multi-factor authentication is used throughout the solution, and this includes Single Sign On features as well as integration with third-party applications, including Microsoft Multi-Factor Authentication (MFA).

Session Management: Implement proper session management techniques such as session timeouts, secure session storage, and session token regeneration to prevent session hijacking and fixation attacks.

Access Control: Implement proper access controls to ensure that users can only access the resources that they are authorized to access. Enforce strong passwords that are at least 8 characters long, include a combination of upper and lowercase letters, numbers, and symbols, and change every 90 days. Secure password storage techniques, like salting and hashing, are used to prevent unauthorized access in case of a data breach.

Secure Communications: Use secure and up-to-date communication protocols such as TLS v1.2 (HTTPS) to ensure that all data transmitted between the client and the server is encrypted and protected with 2048-bit SHA-256 SSL certificates to prevent eavesdropping and/or alteration. Common Alerting Protocol (CAP) messages have XML Digital Signatures created and attached to the messages to maintain the integrity, and SHA-256 hashes of all files (text and audio) are recorded to be used for tamper/integrity comparisons.

Error Handling: Developers should implement proper error handling mechanisms to prevent information disclosure and ensure that error messages do not contain sensitive information that can be used to exploit the application.

Code Review: Regularly review the application code to identify security vulnerabilities and ensure that secure coding practices are followed.

Security Testing: Conduct regular security testing, such as penetration testing and vulnerability scanning to identify and remediate security vulnerabilities before they are exploited by attackers.

User Roles

The following user roles are available in Alertable:

- Basic User: A customer with a basic account. This user can read alerts and reports, and typically issue alerts using templates. Additional permissions can be granted as needed.
- Standard User: A customer with a full account. This user can create alerts and messages, and access all alert-related information and reports.
- Agency Admin User: A customer with management privileges. This user can create alerts, manage accounts, and oversee templates for their agency.
- Super User: An internal PEASI staff member with access to the entire system. Super users can manage accounts, perform all operations, and make temporary system changes.

- System Administrator: An internal PEASI staff member with full control over the system. System administrators can manage all applications and perform any necessary system tasks.

Data Security

Data Security is a critical part of our overall security framework. It is essential for ensuring the confidentiality, integrity, and availability of data, which is a vital asset for our organization. By following these principles and measures, we can ensure that our data is secure, compliant with regulations and industry standards, and continuously improve our security posture.

Data Security Principles

We recognize the importance of safeguarding our customers' data and protecting our own sensitive information. To achieve this, we have established a set of data security principles that serve as the foundation for our data security strategy. These principles outline our commitment to maintaining the confidentiality, integrity, and availability of data across our organization. By adhering to these principles, we can ensure that data is protected at every stage of its lifecycle, from creation to deletion, and mitigate the risks of data breaches or unauthorized access.

- Defence in Depth: Data security measures are implemented at multiple layers, such as network, application, and data levels, to provide overlapping protection.
- Least Privilege: Access to data is restricted to only authorized personnel on a need-to-know basis.
- Separation of Duties: Different roles within our company have different levels of access to data, to prevent a single individual from accessing sensitive data without authorization.
- Data Encryption: Data is encrypted both in transit and at rest using up-to-date methods such as AES-256 to protect against unauthorized access.
    - Full disk encryption: encrypts the entire storage device, including the operating system and all files. This means that even if the device is stolen or physically accessed, the data remains protected.
    - File-level encryption: encrypts individual files and folders. This means that only authorized users with the appropriate key can access the encrypted files.
- Auditing and Monitoring: Regular auditing and monitoring of data security measures should be conducted to identify and address potential security risks.

By following these principles, our company can design and implement an effective data security architecture that protects against potential security threats, ensures compliance with regulations, and provides a foundation for continuous improvement.

Data Security Measures

To protect sensitive data from unauthorized access, loss, or theft, we have established a set of data security measures. These measures include a combination of technical and administrative controls designed to safeguard our data's confidentiality, integrity, and availability. By implementing these measures, we can reduce the risk of data breaches and ensure that our customers and stakeholders can trust us with their information. In this section, we will outline the data security measures that we have put in place to mitigate these risks.

- Data encryption: Encryption is the process of converting data into a code to prevent unauthorized access. Data encryption is implemented both in transit and at rest to protect against potential threats. This measure is also used to protect sensitive data such as passwords and other personal information.

- Access Controls: Access controls are used to restrict access to data and ensure that only authorized personnel can view or modify sensitive information. Access controls include user authentication, role-based access control, brute force protections in the form of account lockouts, login failure alarms, and activity logs including recent user logins, recent alert activity, login failures, and changes to accounts. System alarms are triggered when any errors or suspicious events occur. Default accounts not necessary for the system to function properly are disabled or removed.

- Data Backup and Recovery: Data backups are essential to ensure that data can be restored in the event of a security incident or data loss. We regularly backup all application and customer data to ensure that critical data can be recovered in the event of an emergency. Built-in encryption features are used to encrypt the backup data before it is written to the backup media. The encryption keys are managed by the backup software and stored on a separate server or in a secure database.

- Data Retention Policy: We retain customer data for as long as the customer is an active user of the service. Customer personal data is deleted when the customer terminates their account to comply with privacy regulations.

- Segmentation: The Live, Test, and Development environments and their data are segmented to protect personal and customer information, limit the scope of potential attacks and reduce the impact of any inadvertent changes to data.

By implementing a combination of technical and non-technical data security measures, organizations can protect against potential threats and ensure the confidentiality, integrity, and

availability of data. These measures should be regularly reviewed and updated to ensure that they remain effective against emerging threats.

Information Classification

The appropriate application of security classification is the first step in ensuring the integrity, availability, sensitivity and/or value of data and information. The Government of Canada has established information security classification levels. Provinces and territories in Canada have related standards that align with the national classifications, which support data and information sharing across jurisdictions. The standard describes four data and information security classification levels:

Level	Description
PUBLIC	Applies to data and information that, if compromised, will not result in injury to individuals, governments or to private sector institutions.
PROTECTED A	Applies to data and information that, if compromised, could cause injury to an individual, organization or government.
PROTECTED B	Applies to data and information that, if compromised, could cause serious injury to an individual, organization or government.
PROTECTED C	Applies to data and information that, if compromised, could cause extremely grave injury to an individual, organization or government.

Alertable stores and manages only PUBLIC-level information. Information captured and stored for business users consists of only business contact information, and all alert content is published for consumption by the general public or workforce. Information captured and stored for the public includes the minimum information needed to fulfill the function of the solution, which is to deliver an alert message to the individual. For example, if a member of the public wants to receive alert messages by SMS, then all we capture and store is the mobile number. Similarly, if someone wants to receive alert messages by email, then all we capture and store is the email address. If by mobile app, there is no personally identifiable information captured and stored other than geo-location when the “Follow Me” setting is turned on. There’s no user account needed to be created in the mobile app. Appropriate information access controls are

applied for public-level information in accordance with the security architecture and standards described above.

Personal Information Privacy Considerations

Alertable collects the minimum necessary personal information necessary to deliver emergency alerts and general community notifications to subscribers, perform customer service and support, and inform subscribers about new features and services.

Alertable collects the following information or data:

- Email address
- Phone number
- Unique mobile device ID
- Location information - province, region, municipality, street address, and/or GPS location
- Device information - settings and preferences
- Log Data - Internet Protocol (“IP”) address, computer equipment make and model, operating system version, browser type, time and date of usage

Information collected will vary based on how the user chooses to be notified. For example, an email address is only collected when the user chooses to subscribe to email notifications, a phone number is only collected when the user chooses to subscribe to SMS or Phone (voice) notifications, and so on.

Installing Alertable on various types of devices requires the user to have an account with an applicable service or platform provider. For example, installing the Alertable iOS app requires an Apple ID, and the Android app requires a Google Account. Alertable does not collect any user information from these providers. Instead, we receive a Unique mobile device ID that allows us to send notifications to the device the app is installed on.

Alertable collects data and information from computer equipment and devices called Log Data. This includes the Internet Protocol (“IP”) address, computer equipment and device name, operating system version, the configuration of the Alertable application, the time and date of usage, and other usage statistics. Log Data is used to provide customer support and to gain insights into how to improve features and services.

The table below provides detailed information regarding the justification for the collection of personal information:

Criteria	**Comments**
Is the initiative directly related to and necessary for an organization’s program or	Yes. The initiative is essential to the organization’s emergency program and its

Criteria	Comments
activity?	duty of care to residents, visitors, employees, and students, specifically to provide timely information about threats to their safety.
Is all of the information to be collected directly related to and necessary for the organization's program or activity?	Yes. To deliver crucial, potentially lifesaving information to individuals in their preferred format (e.g. SMS, email, phone call, app) we need a wireless number, email address, phone number or device ID for whom the message can be sent.
Have less intrusive data collection measures been considered that will meet the requirements of the program or activity?	Yes. Alertable is built on the principle of Privacy by Design (PbD). It captures the minimum information needed to fulfill its function and purpose, which is to send crucial information to recipients in their chosen format (e.g. SMS, email, phone call, app).
What problem is the system expected to address?	Alertable solves many problems that emergency managers and communication teams face when having to notify populations and workforces of threats and daily incidents. These include: ● Reaching every corner of the population/workforce, no matter the language spoken, abilities and technology comfort level,s so no one misses out. ● Reaching everyone instantly with time-sensitive information and instructions that can save lives, time and operations. ● Providing comprehensive information for better situational awareness. ● Gaps in the duty to notify obligations of a local official, employer and service provider.
How will the system address this problem?	Alertable provides more ways for people to choose from to receive alerts so that they get information in a format that works best for them. It's 1-click language translation capabilities ensure non-English/French speakers can easily comprehend the messag,e and it is accessibility compliant so that people with different levels of ability can

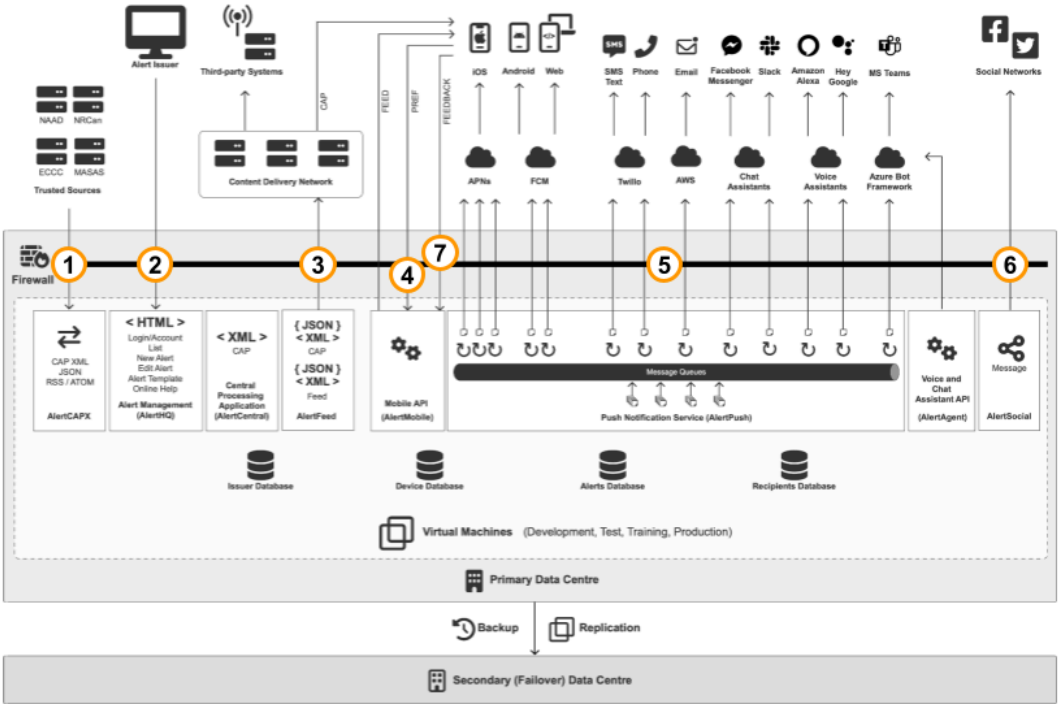
Criteria	Comments
	easily sign up and receive important messages. Alertable is architected to send messages rapidly without compromise or failure.
How will the benefits outweigh any privacy invasion resulting from the use of the system?	The social and economic impact of disasters on communities, businesses and schools can be significant. Alertable helps to protect people and property, to help reduce these impacts.
Will each person about whom information is collected give consent in writing?	To sign up for notification messages provided by the Alertable service, a user must provide their consent to receive notification messages and to share certain information to achieve this (e.g. a wireless number, phone number, email address or device-level information for the app).
Will information about persons be collected directly from the persons themselves and by no other means?	Yes.

Information Flow

This section outlines how both personal and non-personal information flows through the Alertable platform, including sources of data input, internal processing, and output destinations.

Flow of Alert Information (Non-Personal Data)

The diagram below depicts the flow of data through the Alertable platform.



Data flow key highlights (circled in the above diagram) are described below:

1. Alertable gets alert-related information from trusted feeds to external alerting systems like the severe weather alert system from Environment and Climate Change Canada and the national public alert system.

2. Alert issuers (Administrators/Operators) login to Alertable from a browser on any internet-connected desktop computer or mobile device and create an alert message that includes the type of alert they want to send, its severity and description, the geographic area that is impacted by the emergency, and any actions that people should take. Alert issuer credentials are securely stored in databases housed in virtual machines within data centres located in Canada.

3. Alert message content is sent to third-party systems (e.g. roadway signage, community and facility digital displays, other emergency management systems, etc) and recipient Alertable products (e.g. Alertable mobile app, website, etc) through a content delivery network (CDN) to deliver messages to the recipients with the lowest possible latency and the highest possible speed as well as provide additional security benefits such as protection against distributed denial-of-service (DDoS) attacks.

4. Recipients preferences for the types of alerts they want to receive and for what locations are sent to Alertable so they get alerts they want to receive. Recipient preferences are

communicated via a preferences API and stored in databases housed in virtual machines within data centres located in Canada.

5. Alert message notifications are sent to recipients to let them know there is new alert message content.
6. Alert message content is sent to social media, Facebook and Twitter.
7. On supported platforms, recipients respond to alerts. Responses are communicated via a feedback API, and may be comprised of a confirmation receipt, response to a poll question, or engagement with a survey link. Responses are available to Alert issuers (Administrators/Operators), and recorded in databases housed in virtual machines within data centres located in Canada.

Flow of Personal Information

The table below breaks down the flow of personal information to illustrate how personal information moves through the system.

	Description/Purpose	Type
1	Collection of subscriber personal information	Collection
2	We may need to transmit an individual's phone number to a telecommunications provider or send device information to a mobile system provider's notification services to deliver targeted alert notifications. The providers use the information according to their own privacy and regulatory requirements.	Disclosure
3	Emergency alert notifications	Use
4	Contacting subscribers regarding administrative notices, to resolve disputes, troubleshoot problems and enforce the terms and conditions of any agreements.	Use
5	Contacting subscribers regarding administrative notices, to resolve disputes, troubleshoot problems and enforce the terms and conditions of any agreements.	Disclosure
6	Location of user	Collection

Personal Information Risk Mitigation

The following table identifies some potential risks, the strategy to mitigate them as well as their likelihood of occurring and potential impact:

	Risk	Mitigation Strategy	Likelihood	Impact
1	Providing third parties with personal information to deliver emergency notifications	Personal information, including email addresses, phone numbers and device IDs are provided to third-party communications providers such as wireless and mobile device providers for the sole purpose of transmitting notification messages to recipients. Subscribers are made aware of this in the privacy statement, which they consent to upon signing up or downloading.	Medium	Low
2	Use of GPS to track subscribers' movement	Subscribers are made aware of this in the privacy statement, which they consent to upon signing up or downloading. Subscribers must also consent to Alertable accessing device's GPS upon installation of the app.	Medium	Medium
3	Personal information required to provide emergency notification service	The minimum amount of personal information is captured to fulfill the function of Alertable, which is to transmit notification messages to	Low	Medium

	Risk	Mitigation Strategy	Likelihood	Impact
		recipients. This information is limited to email address, phone number and device ID. Subscribers are made aware of this in the privacy statement, which they consent to upon signing up or downloading.		
4	Subscribers provide personal information	The minimum amount of personal information is captured to fulfill the function of Alertable, which is to transmit notification messages to recipients. This information is limited to email address, phone number, and device ID. Subscribers are made aware of this in the privacy statement, which they consent to upon signing up or downloading.	Low	Medium

Network Security

Network security is designed to protect computer networks from unauthorized access, attacks, and other security threats. Network security includes a set of principles and practices aimed at preventing network breaches, reducing the risk of data loss, and ensuring network availability. By implementing a robust network security architecture, we can protect our assets, maintain compliance with regulatory requirements, and safeguard our reputation and that of our customers.

Network Security Principles

We follow network security principles that serve as our fundamental guidelines for ensuring the security and integrity of our network. These principles provide us with a proactive and comprehensive approach to protecting our network against vulnerabilities, unauthorized access, and attacks. We believe that having a well-defined set of network security principles is crucial in establishing a strong foundation for designing, implementing, and managing a secure network. By incorporating these principles into our network security strategy, we can enhance our ability to detect, prevent, and respond to potential security incidents.

- Segmentation: Network segmentation involves dividing the network into smaller, more secure segments or zones, such as the segmentation of Live and Test environments. This principle is essential in limiting the scope of potential network attacks and providing additional layers of security.
- Defence in Depth: Network security measures are implemented at multiple layers, such as network, transport, and application layers, to provide overlapping protection.
- Least Privilege: Access to network resources is restricted to only authorized personnel on a need-to-know basis.
- Secure Configuration: Network devices are configured securely to reduce the risk of security vulnerabilities and ensure proper functionality.
- Regular Auditing and Monitoring: Regular auditing and monitoring of network security measures are conducted to identify and address potential security risks.

Network Security Measures

We understand the importance of implementing effective network security measures to protect our network from cyberattacks and unauthorized access. Network security measures are the practical steps we take to ensure that our network is secure and that the data and resources within it are protected. These measures are designed to safeguard against various types of attacks, such as malware, phishing, and data breaches. By implementing a strong set of network security measures, we mitigate the risk of network security incidents and ensure the confidentiality, integrity, and availability of our network resources.

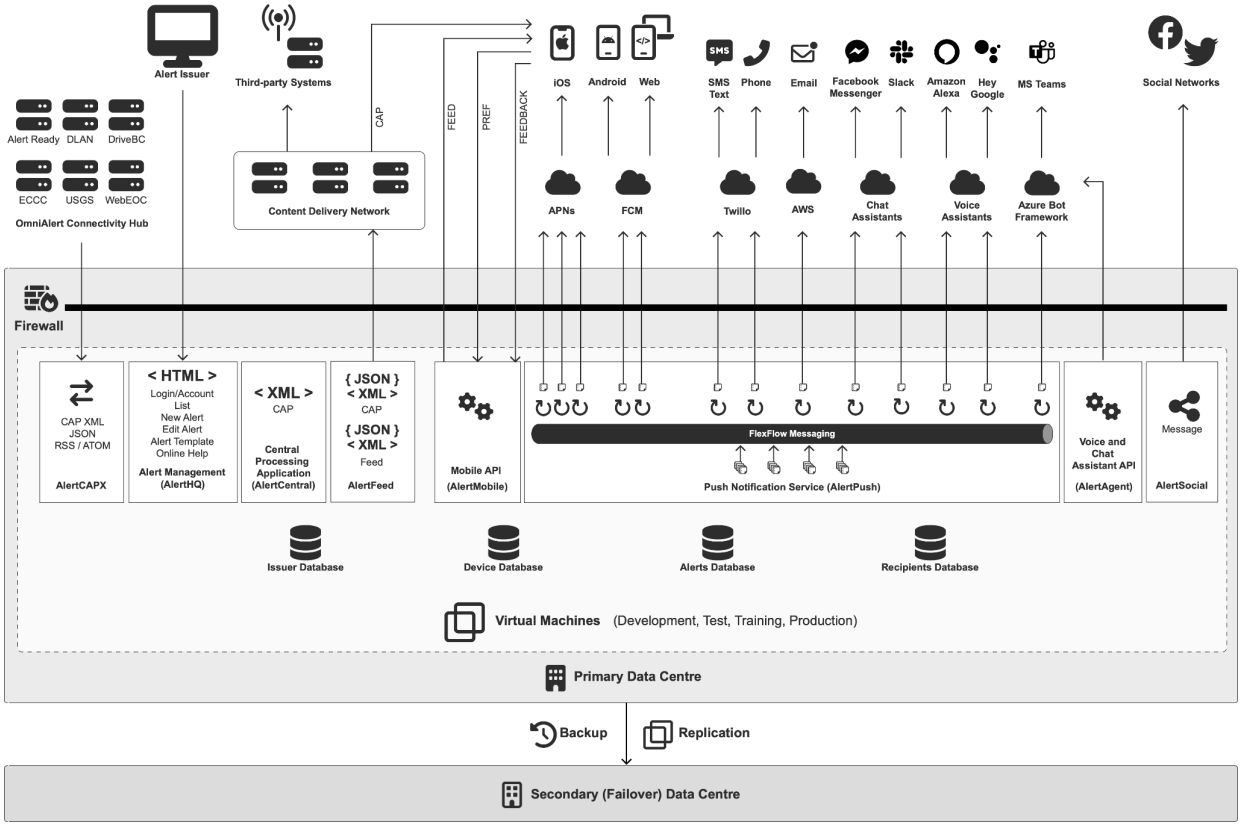
- Firewalls: Firewalls are network security devices that monitor and filter traffic based on predefined security rules. Firewalls are used to prevent unauthorized access and protect against potential network attacks.

- Intrusion Detection and Prevention Systems (IDPS): IDPSs detect and prevent potential network attacks. These systems identify potential network attacks and take action to prevent them from succeeding.
- Virtual Private Networks (VPN): IPsec VPNs are used to create a secure connection between remote users and the organization's network. VPNs provide secure remote access to the network and protect against potential network attacks.
- Network Access Control (NAC): NAC is a security solution that ensures that only authorized devices are allowed to access the network. NAC is used to prevent unauthorized access and protect against potential network attacks.
- Network Segmentation: Network segmentation involves dividing the network into smaller, more secure segments or zones, such as the segmentation of Live and Test environments. This measure limits the scope of potential network attacks and provides additional layers of security.
- Physical Security: Datacentres have implemented secure access to the physical hardware, including fully-secured server cages and 24/7 monitoring.

By following these principles and implementing these measures, organizations can design and implement an effective network security architecture that protects against potential security threats, ensures compliance with regulations, and provides a foundation for continuous improvement.

Network Architecture

Behind the scenes, Alertable is a robust infrastructure designed to provide high-performance throughput of messages, system redundancy and fault tolerance. Characteristics of key infrastructure are provided on the next page.



1. Firewall

- All network communication will be encrypted with HTTPS and IPSec VPN
- A CDN for enhanced performance and DDOS prevention and mitigation
- Enhanced DNS service with Load Balancing
- External security monitoring, alerting and reporting

2. Application Services Virtual Machines

- Intrusion Detection and Prevention are provided by the firewall systems
- All traffic is logged and audited
- Web Application Firewall available

- Regular testing and verification using automated security testing tools

3. Databases

- NIST, CERT, and OWASP best practices followed
- Fine-grained user access control with two-factor authentication supported
- Database transaction auditing and regular snapshots
- Detailed audit log of all user actions

4. Datacentres

- Managed operating systems with up-to-date security patching
- Service and data replication to geographically separate sites to provide high redundancy
- Encryption of data at rest (backups) and in transit
- Defence in-depth access controls to operating systems and hardware
- CSA, SOC 1-2-3, ISO 9001, 27001, 27017, 27018 compliant

Primary hosting services are provided by Amazon Web Services (AWS) in their Canadian data centres:

- AWS Canada West (Calgary) Region: Located in Calgary, AB
- AWS Canada (Central) Region: Located in Montreal, Quebec.

They adhere to numerous industry-standard security and privacy specifications. Certifications are performed by independent third-party auditors EY CertifyPoint, an ISO certifying agent

accredited by the Dutch Accreditation Council, and a member of the International Accreditation Forum (IAF). For more information, see:

- https://aws.amazon.com/compliance/iso-27017-faqs/
- https://aws.amazon.com/compliance/soc-faqs/

Secondary hosting services are provided by Microsoft Azure in their Canadian data centres:

- Canada Central: Located in Toronto, Ontario.
- Canada East: Located in Quebec City, Quebec.

Microsoft also adheres to industry-standard security and privacy specifications. For more information, see:

- https://learn.microsoft.com/en-us/azure/compliance/offerings/

Threat Risk Assessment

Threat Assessment

A list of the most common threats that could potentially affect Alertable.

Threat	Description	Likelihood
T1	Natural disaster – disruption of services due to natural causes ie. flooding, extended power outages, tornado damage, fire, etc.	Low
T2	Human-caused disaster – disruption of services due to human intervention ie. fire, data center flooding, fibre cable cut, etc.	Low
T3	Data centre failure – a significant failure of the data centre infrastructure	Medium
T4	Inside attack – a security exploit or denial of service perpetrated by a disgruntled, negligent, or terminated employee	Low
T5	Malicious customer – a security exploit or denial of service perpetrated by a valid customer	Low

Threat	Description	Likelihood
T6	External attack – a security exploit, virus, or denial of service perpetrated by an external attacker such as a hacker/cracker or criminal/state-sponsored organization	Medium
T7	Eavesdropping – interception or monitoring of sensitive communications	Medium
T8	Contractual breach – a contractual failure either by PEASI or by a party contracted by PEASI	Low
T9	Loss of data – an accidental loss of customer or business data	Medium
T10	Information disclosure – an unintended disclosure of confidential information, data, or user information such as passwords	Medium
T11	Maintenance error – an error that may occur during system administration or maintenance activities	Medium
T12	Communication failure – a disruption in communications between data centres, between staff and the servers, or between staff and customers	Medium
T13	Software errors – a flaw or unexpected condition that causes a software error	High
T14	User error – an action by a user that results in an unintended consequence, such as a service outage	Medium

Vulnerability Assessment

A list of the most common IT vulnerabilities, in general, that could potentially affect Alertable.

Vulnerability	Description	Likelihood
V1	Operating system – flaws in the operating system that are not yet fixed or the patches have not yet been applied	Medium

Vulnerability	Description	Likelihood
V2	Supporting software – flaws in supporting software, such as the web server, database, etc, that are not yet fixed or the patches have not yet been applied	Medium
V3	Password management – poorly chosen passwords or passwords that have not been recently changed	High
V4	Inadequate capacity – not enough capacity for the system to function ie. storage space, CPU or RAM resources, etc.	Low
V5	Change management – inadequate processes in place to manage changes and other operations	Medium
V6	Backups – inadequate or irregular backups, failures in the backup system, or failures in the restore system	Medium
V7	Physical protection – lack of protection for physical server assets from both environmental dangers such as theft, vandalism, etc.	Low
V8	Security awareness – lack of training or processes to ensure staff and customers follow security procedures	Low
V9	Training and supervision – inadequate training and supervision of staff to ensure mistakes are not made	Medium
V10	Software testing – a software testing regime that is not comprehensive and is not able to detect flaws and regressions	Medium
V11	Documentation – lack of documentation on the system and its operation	Medium
V12	Software specifications – incomplete software specifications and design documentation	Low
V13	SQL injection – malicious attacks using SQL special characters and code	Medium
V14	XSS – cross-site scripting attacks using JavaScript	Medium

Controls

A list of risk controls and threat/vulnerability mitigations that have been put into place for Alertable.

Control	Description
C1	OWASP best practices - The Open Web Application Security Project (OWASP) best practices are adhered to, and regular audits using specialized security and penetration tools help to validate this.
C2	Security reviews - A continuous improvement approach to not only new features but also to security is implemented, and an assessment of current and newly emerging risks takes place during regular security reviews.
C3	Login protections - User accounts are protected with an active monitoring system, two-factor authentication methods, brute force protections, and login failure alarms. The solution monitors and logs all activity from authorized users.
C4	User audits - Reports are available that detail recent user logins, recent alert activity, login failures, and changes to user accounts and agencies.
C5	Transport encryption - All applications, including the public-facing websites, use TLS (HTTPS) as the default transport with 2048-bit SHA-256 SSL certificates. An IPSec VPN between all solution servers is used to secure data and services.
C6	Data center security - Intrusion Detection Systems (IDS) and Intrusion Detection and Prevention (IDP) are provided through enterprise-class Juniper SRX firewall hardware. All activities against cloud servers are automatically logged and stored indefinitely. There is no access to physical hardware or the hypervisor layer. The data centres enforce strict "defence in depth" controls to secure access to physical hardware that includes fully-secured server cages and 24/7 monitoring.
C7	Software patching – A regular monthly patch cycle has been implemented to ensure software patching is kept up-to-date.
C8	Security manual – A detailed security manual has been developed for staff and developers to follow that outlines processes, procedures, and best practices.
C9	Penetration testing – Penetration testing is conducted regularly to scan for any weakness, including against new and emerging threats.

Control	Description
C10	Automated software testing – Functional and unit testing of software ensures that requirements are met and no regressions occur.
C11	Server scaling – The cloud platforms have dynamic scaling configured to allow the servers to horizontally scale to handle sudden bursts of traffic.
C12	Backups - Automated daily snapshot backups of the servers take place. All backups are fully encrypted for storage and decrypted upon restoration. Restores can be performed at the file and folder level. Data can be restored from any daily backup performed in the current 14-day window.
C13	Change management - We adhere to the ITIL framework for the delivery of our service and support offerings, and we follow a set of certified ITSM processes and practices. As part of our ITIL service delivery framework, we have developed incident, service request, and change management processes and procedures.
C14	Password policy – The system supports a configurable password policy that can enforce password length and complexity, as well as the regular updating of passwords by users.
C15	Multiple data centres – Our services are hosted in multiple geographically separate data centres. For redundancy, we use separate providers as well.
C15	Simplicity – The software and systems are designed to be simple to use for the end-users and also simple to manage and maintain for the administrators.
C16	Legal agreements – All staff and third-party contractors have performance, confidentiality, and liability agreements. Customers are vetted and must also sign agreements.