Comm100 Live Chat Security Features and Practices

Contents

Introduction

Security is one of the top concerns of enterprise businesses when they are looking to adopt a SaaS solution. A secure SaaS provider requires world-class data centers, stringent identity management and training processes, and rigid security standards.

Comm100 Live Chat is an enterprise-grade live chat application, with security features that perform at the top of the industry. As a SaaS and customer-driven company, we know the true challenges of providing quality and secure live chat services, inside and out.

We have policies and practices that address a whole range of security concerns, building off of a solid foundation that helps our clients exceed their customers' expectations.

In this security white paper, we present a detailed and comprehensive report on our security processes and standards. Through this we hope not only to prove our commitment to protecting our customers' data, but also explain how we keep our application safe from cyber threats.

Application Security

Comm100 Live Chat allows agents to monitor and engage visitors, as well as obtain crucial information regarding their purchasing and website surfing habits. The security measures at the application level help keep this sensitive data guarded from online threats.

HTTPS Encryption

When a chat connection is built, all data collected from visitors via multiple forms (i.e. browsers, pre- chat, post chat survey), as well as chat messages transmitted between live chat agents and visitors, is encrypted through HTTPS protocols utilizing the advanced TLS encryption.

Credit Card Masking

With the Credit Card Masking feature enabled, credit card numbers that are sent by visitors directly through chat window to agents will be automatically masked and kept private. Instead, you can use the PCI DSS compliant Secure Form to collect sensitive information from visitors during chatting.

PCI DSS Compliant Secure Form

Our PCI DSS compliant Secure Form allows you to request sensitive data such as credit card number from visitors through the chat window. This data will not be stored in our database, and agents can only access the data during the chat session. Once the chat session ends, both agents and visitors cannot re- access the data. The Secure Form is certified for PCI DSS compliance. If your business is PCI DSS compliant and you use our Secure Form to collect credit card holder data during the chats, you will stay compliant without additional audits or expenses.

IP Restrictions

You can authorize specific IPs or IP ranges for your Comm100 Live Chat account. This limits agents to access their accounts from designated IPs. IP restrictions can also be enabled for mobile access.

Password Security

Passwords are a crucial and an often-overlooked component of data security – as a result, they can be particularly vulnerable to attacks. Comm100 Live Chat's password security system contains the following features:

- HTTPS authentication
- All passwords are authenticated by HTTPS.
- Password encryption
- All passwords stored in company databases are kept private through irreversible encryption.
- Password complexity standards

  Passwords are required to meet certain complexity requirements as set by users. Customizable password requirements for agents include:

  - Number of characters
  - Character type requirements, such as uppercase, lowercase, numeric and special (such as $, &, #, @, etc.)
  - Common phrases not allowed (i.e. 123456, password, qwerty, etc.)
  - Username not allowed
  - Password expiration time
  - Password change frequency
  - Password reset limits
- CAPTCHA and account lockout

  If the incorrect password is entered for an agent's account five consecutive times, CAPTCHA verification is enabled to prevent malicious attacks.

  Account lock-out can also be enabled after a predefined times of failed login attempts.

Session-Only Cookies

While agents are logged into their live chat accounts, Secure and Http Only flags are set in the session-only cookies to ensure account security.

Agent Permission Setting

Agents can be assigned customizable permission settings. This limits the actions agents can take as management finds appropriate.

Permissions can also be granted at department and group levels.

Permission tasks include, but are not limited to:

- Accepting chats
- Refusing chats
- Joining chats
- Transferring chats
- Chatting with other agents
- Monitoring chats
- Inviting visitors to chat
- Viewing department's transcripts and offline messages
- Viewing all chat transcripts and offline messages
- Deleting transcripts
- Viewing reports
- Managing campaigns (customization)
- Managing canned messages
- Managing ban list

- Managing routing and allocation rules
- Managing security settings
- Managing agents, departments, visitor segments, custom variables and many others

Agent Audit Logs

All agent activities can be tracked through audit logs, providing management with accountability for all actions performed within the application.

You can track information in the audit logs by time period, keyword, and filter for time-sensitive resolutions. Through permission settings, access to audit logs can be restricted to administration and trusted agents.

Infrastructure Security

A quality live chat application requires the most secure infrastructure possible.

Comm100 Live Chat is committed to only the best, most advanced procedures and policies to keep the foundation of our operations secure.

HIPAA Compliance

Comm100 offers HIPAA compliant live chat as a Business Associate under the Health Insurance Portability and Accountability Act of 1996. Our live chat system has been fully assessed to ensure that electronic Personal Health Information (ePHI) is kept secure: All live chat data is fully encrypted, we operate strong firewalls and DDoS protection, and we have additional security measures which ensure that the process of logging into and operating our system is fully compliant.

We comply with the highest levels of infrastructure security to ensure that our live chat is HIPAA compliant. We have undertaken extensive system hardening and network security practices, and operate penetration and vulnerability tests to ensure that we remain compliant. Some of the safeguards and processes we operate to check and maintain compliance include:

- System monitoring & notification processes
- Intrusion detection system
- Quarterly internal and external vulnerability scan

- Quarterly network segmentation testing
- Yearly penetration testing

ISO 27001 Certification

Comm100 has achieved ISO 27001 certification, the international standard which defines best practices within an Information Security Management System (ISMS). Compliance with this standard confirms that Comm100 has compliant governing processes over all hardware, software, people and procedures in accordance with internationally-recognized standards.

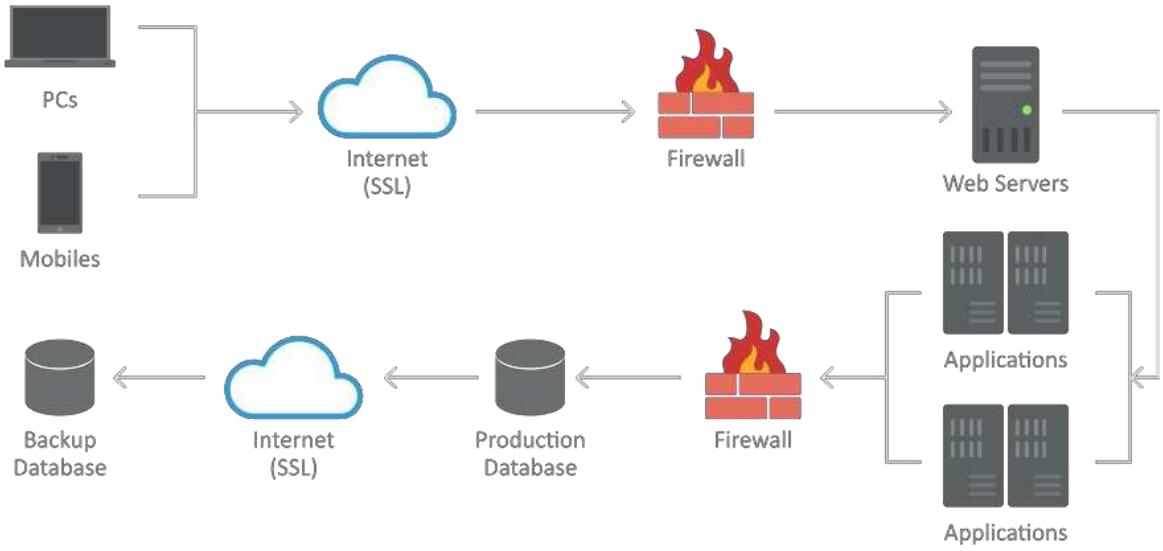
PCI DSS Compliance

Comm100 Live Chat is PCI DSS compliant as a service provider. PCI DSS (The Payment Card Industry Data Security Standard) is a proprietary information security standard for organizations that handle branded credit cards from the major card companies including Visa, MasterCard, American Express, Discover, and JCB.

Being PCI DSS compliant, we are enforcing the industry leading security controls over the physical environment and all procedures and processes governing our software development, deployment and operation. Our security management is fully repeatable, defined and consistent.

Network Security

Beginning with the very first point of contact, strong security measures are put in place. All chat requests are validated through a third-party firewall. This ensures that only legitimate chat requests will be accepted, so that the security of the host website will not be compromised.



Server Hardening

All our servers, including chat servers, application servers, and database servers, together with our switches and firewalls, are hardened complying with relevant standards, including Windows server hardening standards, IIS hardening standards, etc.

Anti-Virus Solution

An up-to-date, industry accepted anti-virus solution is critical for successful operations. Comm100 Live Chat has an anti-virus solution that is properly implemented and kept up-to-date. Additionally, all staff members who may have access to the production environment have active and enabled anti-virus on their PCs.

Security Patches

Crucial security patches that call for immediate action will be installed within 30 days of patch release. Non-crucial security patches will follow periodic review on a monthly basis, and are applied only after thorough assessment. Additionally, all security patches are immediately installed when setting up a new server.

To ensure top quality, all patching and software updates must pass rigorous testing before a CAB (Change Advisory Board) committee approval.

Physical Security and Continuing Operations

HIPAA Compliance

We operate HIPAA compliant servers in the US. Our disaster recovery processes are also HIPAA compliant, and alongside these we have a full suite of policies designed to ensure HIPAA compliant levels of physical security.

ISO 27001 Certification

Comm100 is ISO 27001 certified. The ISO 27001 standard lays out the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. It sets a risk-based approach that focuses on adequate and proportionate security controls that protect information assets and give confidence to stakeholders.

Data Centers

Comm100 Live Chat is partnered with recognized industry leaders such as Rogers, Peer1 and UK2Group. The data centers were chosen based off of their commitment to uptime, redundant power sources, and top security features. Our partner data centers pride themselves in:

- Network redundancy
- Power backup
- Secure facilities
- Redundant cooling systems
- Climate control
- CCTV monitoring
- Biometric security features

Our servers are stored separately from others in the data centers to ensure maximum security and privacy. Access to the company's servers are carefully monitored and recorded for review as necessary.

Disaster Recovery

Comm100 Live Chat's disaster recovery environment ensures continuity for clients, supporting all applications, services and components as they function in the production environment. Every change which passes through the CAB committee review will be performed in both the production and disaster recovery environments.

In the event of a regional disaster disrupting the normal production environment, data backups will be automatically restored to the disaster recovery environment and the service can be up and running in minutes.

Processes and Procedures

Comm100 is ISO 27001 certified, and Comm100 Live Chat is PCI DSS compliant as a service provider. We comply with strict standards regarding processes and procedures in our daily operations.

HIPAA Compliance

To achieve HIPAA compliance, Comm100 examined all existing policies and procedures relating to application, infrastructure and physical security and updated them to ensure they encompass the full suite of requirements that HIPAA compliance demands. Some of the relevant policies and processes we have in place include:

- Access control procedures
- Security incident response procedures
- Change management procedures
- Secure development procedures
- Disposal procedures
- Security awareness training procedures

Change Management Measures

Changes at the foundational level are managed under regulated operations detailed in our Change Management Process.

Examples of the changes covered include (but are not limited to):

- Installation of hardware and network equipment
- Uninstallation and configuration adjustment
- Modification of domain and IP
- Upgrade of software and operating system
- Release of product update

In addition, we have employed explicit permission management regarding the login authority to our database. Any operation that may harm our database security is strictly prohibited.

Internal Development Training

Operational security strategies are only as strong as the team that implements them. Our internal development training covers:

- Project development process
- Coding standards
- Web security

Job Role Management

PCI DSS defines the specific permissions and duties of different roles in a company's security team. At Comm100, we strictly follow certain standards in our daily security operations.

- IT Manager is responsible for overseeing all aspects of information security.
- The IT Team shall maintain daily administrative and technical operational security proceduresthat are consistent with the PCI-DSS.
- The Human Resources Office is responsible for tracking employee participation in the securityawareness program
- Internal Audit is responsible for executing a risk assessment process that identifies threats,vulnerabilities, and results in a formal risk assessment.
- General Counsel will ensure that for service providers with whom cardholder information isshared.

Incident Response

Comm100 Live Chat has a complete incident response plan in place to ensure business continuity. Alarm tools are implemented to identify any potential incident.

Our Information Security Team will be notified immediately of any suspected or real security incidents involving our computing assets, particularly any critical system or system that handles or processes cardholder or other Personally Identifiable Information. Incidents will then be classified into different

levels and be taken care of according to specific procedures.

Access Control

Access to our servers and databases is strictly controlled by:

- Password length, complexity and lifespan
- Account activity
- Staff turnover
- Job role management
- Remote access authentication
- Session activity

24/7 Service Monitoring

Comm100's Service Maintenance team monitors the application round the clock, ensuring that potential risks are noticed and acted upon immediately.

Conclusion

As a live chat provider for companies and organizations around the globe, Comm100 Live Chat sets the highest possible standards for how sensitive data is handled. We hope this document serves to inform you about our processes and protocols, as well as about our unwavering commitment to security.

About Comm100

Comm100 Network Corporation is an award-winning global provider of enterprise live chat solution. Comm100 Live Chat is used by thousands of businesses worldwide to support their website visitors in real time so as to increase conversions, boost customer satisfaction and lower operating costs. With "100% communication, 100% success" as the company motto, Comm100 is committed to ensuring that transitioning human-to-human interactions to real-life success stories is always possible in a digital world.

Customers

Accreditations

Contact Us

TEL | (778) 785-0464

Fax | (888) 837-2011

Follow us on |

E-Mail | sales@comm100.com

Web | www. comm100.com

Suite 238 – 1027 David Street Vancouver, British Columbia V6E 4L2 Canada