Security Documentation myConferenceSuite

Contact
Greg Rothwell
gregr@desystems.com
613-723-1166 ext 202

myConferenceSuite Security Information Sheet

Application Overview:

D.E. Systems' myConferenceSuite application is a cloud computing based solution residing on our own Virtual Web server, fully PCI compliant for third party transaction processing. Data is stored in Canada on our own dedicated servers.

KEY INFO

Your Data and General Terms and Conditions

Uptime – D. E. Systems warrants that the myConferenceSuite server is available for operation 98% of all minutes in a year. D. E. Systems provides annual up-time statistics on its web site. In case of any scheduled downtime, D. E. Systems will notify Client at least 24 hours in advance.

Data security – D. E. Systems warrants that it will exercise all reasonable effort and pre-emptive caution to ensure its server is not compromised by viruses or intrusions. To this extent, D. E. Systems ensures latest known vulnerabilities in its server installation are patched and DDOS attacks are averted.

Personal Data - D.E. Systems' Event Management System (myConferenceSuite) is responsible for personal information under its control. Collection of personal information by myConferenceSuite will be limited to what is necessary for the purposes of registration for the event.

Ownership – D. E. Systems warrants that the Client is the owner of all content maintained with myConferenceSuite software, including design templates, logos, text and other content rendered on the Client web site. This entails that on termination of this Agreement, the Client may migrate content from D.E. Systems software to any other data format. D. E. Systems will ensure that the Content will be available for this purpose from a recent backup. Client may elect to have data removed from the platform upon request at any time

Resulting Harm - Client acknowledges that they are solely responsible for the content maintained with myConferenceSuite software and are liable for any harm that may result from the client publishing this content, in particular in the event of fraud, or content of illegal or insulting nature of any kind. D. E. Systems reserves the right to suspend a myConferenceSuite account if improper use by the client of myConferenceSuite software has been reported. It is the Client's obligation and responsibility to monitor content of the Client web site for such improper use and in the case of revenues collected, adhere to any applicable tax law. If the software does not function as warranted, D. E. Systems' liability for any loss or harm shall be restricted to the amount of the contracted service and shall not be liable for any item of so-called consequential loss. In the event of any unauthorized intrusion, data breach or compromise of client data D. E. Systems will notify client immediately of any such compromise to their data.

PCI Assessment

MyConferenceSuite is PCI DSS V 4.- SAQ D compliant.
Attestation Completion Date. March 18, 2025

A copy of this Assessment is available upon request.

Encryption and Authentication: TLS Protocol V 1.3

Data Centre Infrastructure and Security

Dedicated Servers:
E5Xeon
Redundant Drives and RAID
Software/Hardware RAID 100% network uptime SLA
Server management
Free hardware replacement
Available control panels
Full root access
Software installation and setup
Remote reboot
Online backup
Dell PowerEdge servers
SuperMicro servers
Juniper firewalls
SATA/SAS/SSD hard drives
IPMI server monitoring
Remote reboot & console access

Backups:
Data Isolation
Dedicated Backup Hardware
Continuous data backups
Full and Incremental backups
4TB Storage
RAID 1 (Mirror)
Optional Web UI
Database Backup (MySQL, MS SQL)

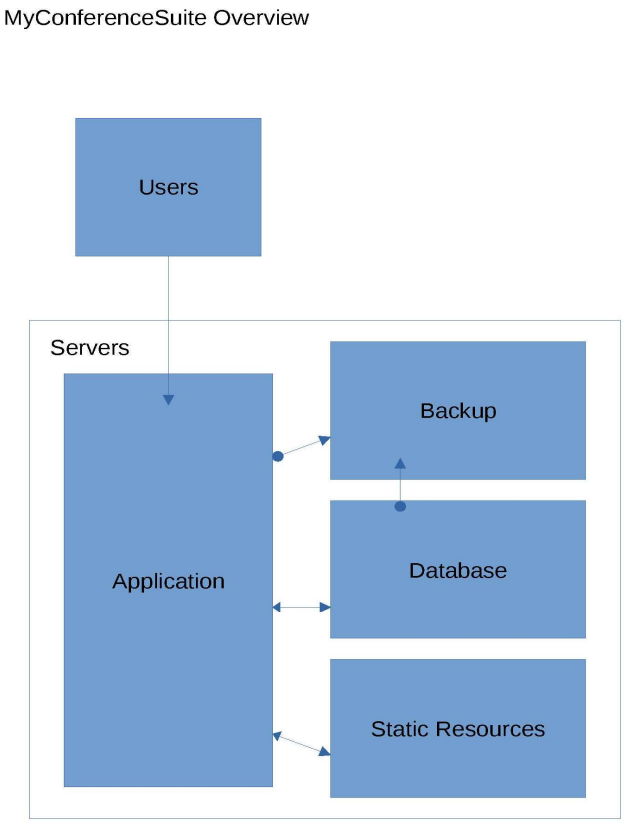
Data backups set to run daily isolated from all other users in the data centre with 256 bit AES Encryption but there is real time data recovery included as well.

Data Centre Certifications and Practices

Data for MyConferenceSuite is stored at Data Centre Canadian Web Hosting. This data centre has completed SOC2 Type 2-Audit of Internal Controls. List of Certifications and Compliance:

- SOC2 Type II certification
- Implementation of ISO27002 guidelines
- Full PIPEDA compliance
- 100% PHIPA (Personal Health Information Protection Act) compliance
- CSA Star Registered-Cloud Security Alliance
- SSAE 16 compliant

Data Flow



Internal Device Security and Procedures

Network Security

- Firewall is configured and actively monitored
- VLANs are used to segment sensitive data/devices (e.g. guest vs internal traffic)
- Intrusion Detection/Prevention Systems (IDS/IPS) are in place
- Network monitoring tools are deployed to detect anomalies
- DNS filtering is used to block malicious sites

Endpoint Protection

- All company devices have antivirus/anti-malware software
- Devices are enrolled in an **Endpoint Detection & Response** (EDR) solution
- Operating systems and software are patched regularly

User Access Controls

- Role-Based Access Control (RBAC)** is implemented
- Multi-Factor Authentication (MFA)** is enabled for all users
- Local admin rights are restricted and logged
- Regular access reviews are conducted (e.g., quarterly)
- Former employees' accounts are promptly deactivated

Email & Communication Security

- Spam and phishing filters are active (e.g. Microsoft Defender for O365, Proofpoint)
- Email encryption is enabled for sensitive communications
- Domain-based message authentication (SPF, DKIM, DMARC) is configured via DNS
- End users are trained to recognize phishing

Authentication & Identity

- Password policies enforce length, complexity, and expiration
- Monitor for unusual login locations or times
- MFA is required for VPN and cloud services

Data Security & Backups

- Regular backups are performed (on-site and off-site/cloud)
- Backups are encrypted and tested regularly
- Data Loss Prevention (DLP) tools are active
- Sensitive files are encrypted at rest and in transit
- Cloud storage is access-controlled and monitored

Software & Patch Management

- OS and applications are updated automatically or via patch management
- Unsupported software and legacy systems are removed or isolated
- Audit of installed software is conducted regularly

Physical Security

- Server rooms are locked and access-controlled
- Security cameras are installed where appropriate
- Hardware inventory is tracked and tagged

Policy & Awareness

- Acceptable Use Policy (AUP) is in place and signed
- Security awareness training is conducted at least annually
- Incident response plan is documented and tested
- Employees know how to report security incidents
- Confidentiality agreements are signed by all staff

Monitoring & Incident Response

- Logs are collected and stored securely
- Regular vulnerability scans and/or penetration testing is scheduled
- An assigned team or contact handles IT security incidents

OTHER Security mechanisms utilized.

- Cyber insurance is in place
- Regular audits (internal or external) are performed
- Business continuity & disaster recovery plans are up to date