COMMERCIAL IN CONFIDENCE

EventsAIR Technical and Organizational Measures for Data Protection and Privacy

Version	Date	Author
0.1	January 29, 2018	Klaus Petrat
0.2	February 1, 2018	Trevor Gardiner
0.3	February 7, 2018	Klaus Petrat
0.4	February 13, 2018	Trevor Gardiner
1.0	February 14. 2018	Trevor Gardiner
1.1	April 2018	Klaus Petrat
1.2	July 2018	Changed Logo
1.3	July 2018	More EA GDPR Features
1.4	November 2018	PCI Perimeter Testing
1.5	January 2019	Physical Security Statement added
1.6	March 2019	System Components and Asset Management
1.9	April 2019	Removable Devices (Already part of annual training but now also part of employment contract and this document)
2.0	June 2019	Mobile App Security Added.
2.1	July 2019	Updated any reference to SSL to TLS 1.2 or higher. Updated OS patching advice. Update Incident – Response plan to 8 hour response after discovery of incident. Updated Password policy to include special character.
2.2	August 2019	Extended Password Policy Setup in EventsAIR.
2.3	August 2019	High Level Component Diagram included.
2.4	September 20 2019	The scope of the Incident Response plan covers all security (beyond just payment card industry related) incidents as well as all privacy breach incidents (GDPR)
2.5	October 30 2019	New process regarding data exports requested by the client.
2.6	TEMPORARY https://devblogs.microsoft.com/azuregov/data-security-qa-with-john-molesky-azure-security-engineering/ Advanced Threat protection https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/	NIST 800-88
3.0	January 2020	Extended with Acceptable Use Policy

3.1	September 2020	In the section Risk, changed staff training from “periodically trained” to “trained annually”
3.1	September 2020	Added SNORT to logging systems to be secured in an assumed breach.
3.2	October 2020	Live replication added to Business continuity

Staff Security Controls, Policies and Procedures

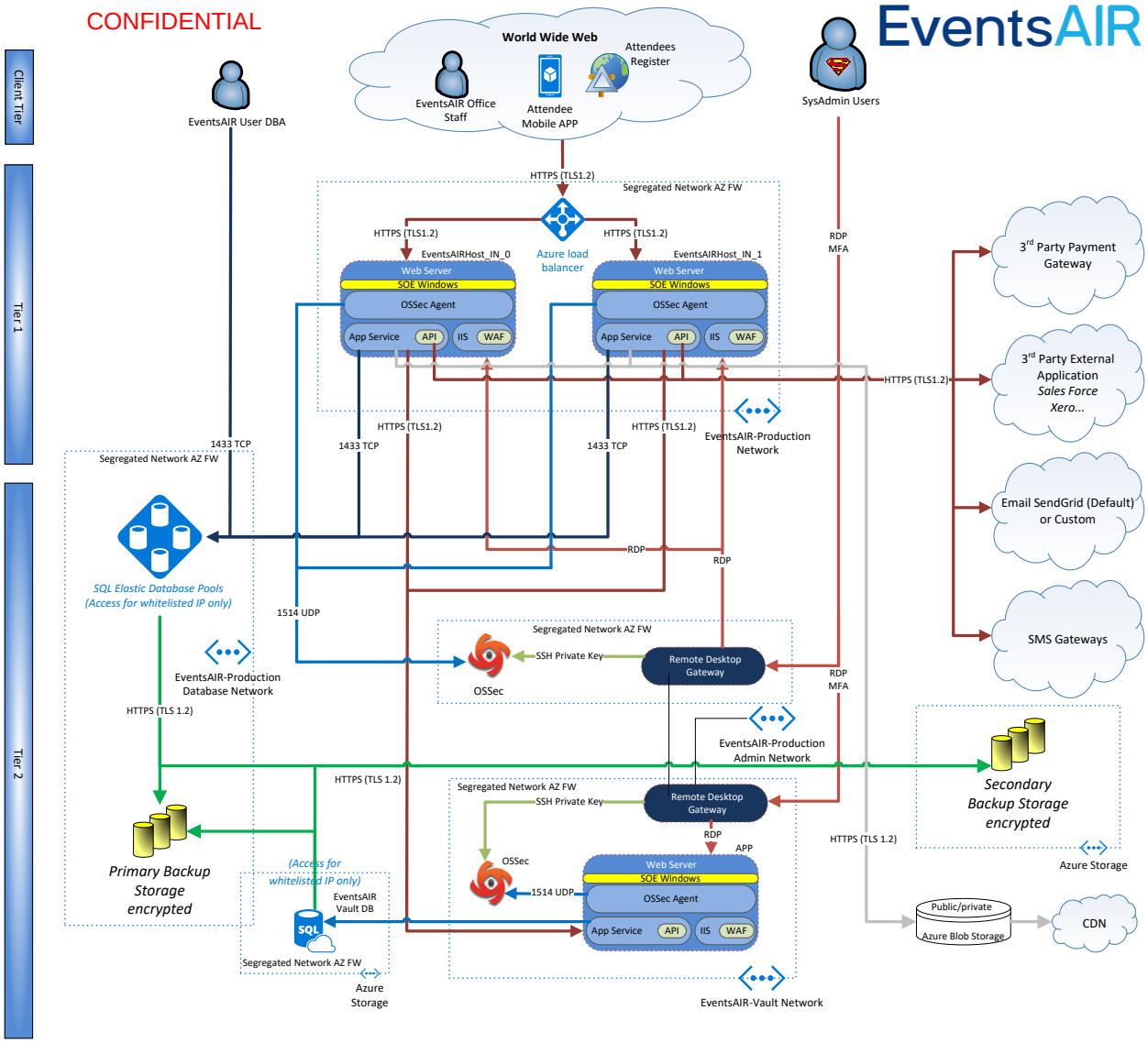
Overview

Professional staff are at the center of Centium Software and encompass Software Developers, QA Staff, Support Staff, IT, Sales & Marketing Staff, Financial Staff, Operational Staff and Administrative Staff.

Since threats, vulnerabilities and hacker attacks continuously evolve, Centium Software has partnered with Microsoft Azure to implement and maintain a holistic approach to security management.

This process also includes staff checks, monitoring and education. For this reason, Centium Software has implemented a series of policies and procedures to ensure that all staff can be fully entrusted in all operations and contribute to the security requirements of our clients' EventsAIR implementations.

A high-level component diagram of the complete EventsAIR architecture is shown below.



Centium Software Staff Security Controls

Staff Contracts

Our staff contracts clearly articulate our security and privacy commitments to our customers.

Security & Awareness Training

Our annual, mandatory staff security and privacy awareness training reflects our compliance with the PCI DSS Level 1 certification, as well as the European Union General Data Protection Regulations (GDPR).

System Access

All staff access to customer production data is secured on a need to know basis. For authorized staff, this includes documented security policies, and access to production data and cloud services is unique and requires dual factor authentication.

All access is logged in a centralized and secured logging server using OSSEC.

Password Policy Enforcement

- All Staff are forced to change passwords every 90 days.
- If any staff makes six unsuccessful attempts within a 30-minute period, that user is locked out for 30 minutes.
- At least 7 characters, 1 numeric, 1 alpha minimum and 1 special character.
- History of last 4 passwords can’t be repeated.

Centium Software Staff Policies and Procedures

Acceptable Use Policies

EventsAIR's management reason for publishing an Acceptable Use standard is not to impose restrictions that are contrary to the EventsAIR established culture of openness, trust and integrity. EventsAIR is committed to protecting its employees and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/intranet/extranet-related systems, including but not limited to IT assets, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, various business applications, web browsing, etc., are the property of EventsAIR. These systems are only to be used for business purposes in serving the interests of the company and of our clients and customers in the course of normal operations.

Effective security and due care of the EventsAIR IT assets is a team effort involving the participation and support of every employee and contractor who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Prohibited Use

Under no circumstances is an employee of EventsAIR authorized to engage in any activity that is illegal under local, state, federal or international law while using company–owned resources. The use of abusive, vulgar or objectionable language on the internet is unacceptable. Additionally, using the internet for the intentional harassment or harm of an individual or organization is prohibited.

Social Media

The use of social media sites and the publishing of blogs, tweets and personal opinions on these sites carry certain responsibilities. Employees are to refrain from comments that can be interpreted as slurs, demeaning, inflammatory, etc. Respect the audience. Don't use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in EventsAIR's workplace. Employees should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory—such as politics and religion.

EventsAIR can and will monitor employee use of social media and social networking web sites, even if the employee is engaging in social networking or social media use away from the office. Derogatory comments about the company or individual employees within the company are not acceptable under any circumstances and such action will result in disciplinary proceedings against any employee found to have posted such content.

Right to Monitor

EventsAIR retains the right to monitor employee activities; management will monitor and audit internet access for the purposes of assuring system security, proper usage and for performance impact. The employee has no rights to privacy in the use of the internet.

Discipline

Failure to follow the Email and Internet Usage Policy or the Information Security Policy will lead to disciplinary action against the employee concerned, which may include reprimand, loss of internet access, suspension, termination or prosecution.

Staff Contracts

Upon joining Centium Software, every staff member is required to sign the Centium Software Employment Contract, containing provisions for Confidentiality regarding client data.

- Compliance with all the relevant laws
  - The Employee will at all times comply with all relevant laws (including any amendments from time to time). These laws include, but are not limited to, workplace health and safety laws, anti-discrimination laws, privacy laws and the corporations law.
  - If the Employee breaches any provision of any law that seriously places at risk the health of any person, whether reckless or deliberate, or is a serious and intentional act of discrimination or harassment the Employee's employment may be terminated immediately without notice.
  - The Employee must take all appropriate steps to familiarize him or herself with all relevant laws that must be complied with.
  - The Employee must immediately notify the Employer of any event that may be or may lead to a breach of any law for which the Employee becomes or ought to be aware.
- Compliance with Privacy Policy
  - The Employee will at all times comply with the Employer's Privacy Policy and any other policies of the Employer (including any amendments thereto) as may be in place from time to time ("the policies").

    If the Employee breaches any provision of the policies, the Employee's employment may be terminated immediately without notice.
  - The Employee must immediately notify the Employer of any event that may be or may lead to a breach of the policies or which the Employee becomes or ought to be aware.
- Mandatory Staff Training (annually)

  Centium Software conducts 2 types of mandatory annual training of staff:
  - Security and Privacy awareness training. This is mandatory to attend and attested by way of staff signature, that the security and privacy awareness training was completed.
  - Annual top ten, certified OWASP training for developers. The top ten threats are continuously updated to reflect the up to date threats which can affect online users.
- Removable Devices

  Removable devices cover both privately and Centium owned laptops, Memory sticks, removable hard disks, CD burners and other devices, on which a Centium Employee could store EventsAIR customer data and/or data owned by Centium Software.

  Under no circumstances will it be necessary for support staff, sales staff or any employee to store customer data on a removable device.

  Removable devices are often not protected and can be accidentally or intentionally left in public places.

  For this reason, storing customer data on such a device will have severe consequences which may end in termination of employment.

  The policy is part of "The annual Security & Privacy Training" pointed this out and it has been signed by all participants.
- Client Request for Data

  In some instances, clients will request raw data extracts from the database and get the output sent as a csv file.

- First, staff is required to verify that the request originates from the client and not a random person. Even if the requesting client user is known but uses a private email such as Hotmail, Google Mail or Yahoo etc., do not send the data.
- Place the CSV or any other output format into the client's AIR Drive and notify via email.

Software Development

EventsAIR was written as a Microsoft Azure cloud service from the outset. This represents a very tight integration between MS Azure and EventsAIR, allowing our clients to take advantage of the Microsoft Azure superior threat monitoring and mitigation capabilities.

Centium Software's software development processes adhere to industry best practice software development life cycle (SDLC) guidelines in developing EventsAIR. It includes:

- Centium Software Custom Application Code Change Reviews Policy and Procedures.
- Centium Software Development Secure Coding Guidelines and Training Policy and Procedures.
- Centium Software Development Life Cycle Processes Policy.
- Centium Software Change Control Policy and Procedures v1.2.
- All code changes are documented in Jira and subject to peer review.
- Change Control Process and Change to System Components

Centium Software maintains the following processes to adhere to strict change control management. These include:

- Development/test environments are separate from production environments with access control in place to enforce separation.
- No client production data is used in the test or development environment.
- A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. QA/Test and support staff do not have access to the production environment.
- Change control procedures related to implementing security patches and software modifications are documented.

Staff Access to Production Data

Centium Software maintains strict separation between staff who have access to production systems and staff who have not. The guiding principle is on a 'need to know and least privilege' basis.

- The user access process provides for who requires access to what, what purpose and for how long.
- All access granted/revoked is documented and requires a formal approval process.
- Only a selected few senior staff have access to production data, solely for client support if required.

Staff Departure and Role Changes

Centium Software maintains strict staff turnover procedures.

- Staff Hire
  - Criminal background checks.
  - Induction orientation, physical access to the building.
  - Access to systems approval process and documentation. Access is given on a needs basis.
- Staff Departure
  - Off boarding process. Deactivate Email and login.
  - Collect physical assets.
  - Change critical passwords.
  - Remove all remote access.
  - Cycle encryption keys where necessary.
  - Document and sign actions taken.
- Staff Role Change
  - Approve document change.
  - Remove existing systems access.
  - Grant required system access.

EventsAIR Cloud App Security Controls, Policies and Procedures

Overview

Centium Software clients access the following apps and databases:

- EventsAIR Cloud App - the desktop app used to manage all aspects of event management.
- Mobile Attendee/Exhibitor Apps - available as HTML 5, native Android and native IOS apps.
- Online HTML5 sites - generated using the EventsAIR Cloud App.
- Custom HTML5 Sites (bespoke development).
- Custom APIs.

Database access for these clients will always only occur via the EventsAIR application server, over port 443 (TLS 1.2 or higher). No client direct access to the database is possible with the exception of a direct SQL Database connection which can be provided to customers who wish to use their own reporting tools.

If a direct SQL Database connection is requested by a client, access is always:

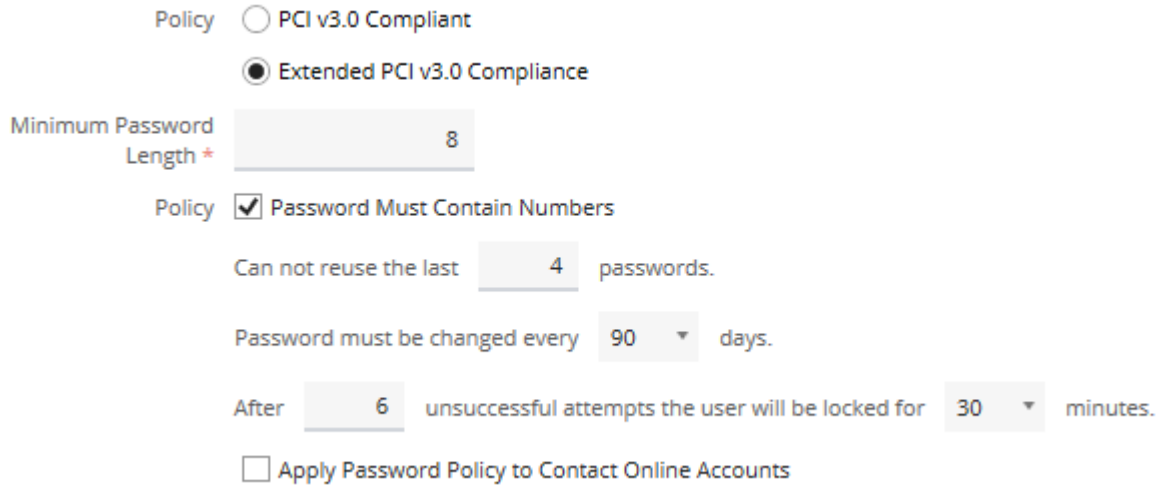
- READ ONLY.
- The IP, from which access occurs, will be whitelisted in the Microsoft Azure firewall.

EventsAIR Client Security/Operational Controls

Client Access

EventsAIR features access controls in several ways and most of these are modelled on the PCI DSS Level 1 compliance requirements:

- Password length minimum 7 characters, at least 1 numeric, 1 alpha character and 1 special character, forced password change after 90 days, no repeat password use for 4 consecutive password changes, lockout after 6 unsuccessful attempts for a 30-minute period, logging to the centralized OSSEC server. Extended password policies may be set up in EventsAIR using the Password policy screen shown below.



- Role based access to various EventsAIR modules. Our customers (data controllers) are responsible for determining the access needs and privilege assignments for each user's role and granting or revoking access to these roles.
- Unique user access IDs for each user

TLS 1.2 or higher

- Centium Software uses strong cryptography and security controls to safeguard data during transmission and at rest. Only transmission with the TLS 1.2 or higher protocol is supported. The EventsAIR cloud app and the EventsAIR registrations sites, which are built using the client, allow only for access to the middle tier via secure communication over port 443. This means, all data, collected and transmitted from the clients to the middle tier, is protected.

Automated Alert Systems

- The EventsAIR cloud app allows the easy building of complex registration web sites by event organizer staff.

  Online sites are one of the most important tools in event management and therefore require special monitoring of availability during the entire registration process. For this reason, Centium Software utilizes StatusCake as well as internal monitoring systems to monitor online sites on a 24/7 basis.

  When sites are offline, automated SMS are sent to Centium Software IT and problem resolution is initiated immediately.

GDPR Data Protection Toolkit

Please refer to http://help.eventsair.com/data-protection-intro

- **Rights to Erasure ('Right to be Forgotten')**

  EventsAIR will allow the data controller (EventsAIR Customers) to either Delete or Anonymize data marked as personal data. EventsAIR only retains and encrypts the minimum personal data required for compliance with other legal obligations. Anonymized data is only accessible by the designated Data Protection Officer who is given access to view the records.

- **Data Administrator (DPO in GDPR)**

  EventsAIR allows our Customers to designate a selected user account as Data Administrator in the user profile. This access will allow the Data Administrator to read anonymized data in clear text, without the ability to alter that data, when performing a search within EventsAIR.

  Only the DPO can view anonymized records.

- **Archiving**

  EventsAIR will allow our Customers to archive events. Only minimum personal data is retained and anonymized for requirements of compliance with other legal obligations. Such data is only accessible by the designated Data Administrator who is given the access to view the records. The action is irreversible.

- **Delete Events**

  EventsAIR will allow our Customers to delete any unused or closed events. All personal data is deleted. The action is irreversible.

- **Access Activities Log**

  In addition to the standard EventsAIR Change Log, the Data Processing Log, logs actions regarding:

  - Consent given, consent withdrawn.
  - Data transmitted to third parties.
  - Notifications to 3rd parties when consent is withdrawn.

- **Contact Locator**

  This serves several purposes:

  - When a data subject demands to view/correct personal data, with the Contact Locator, the data controller can create a Data Processing Statement for the subject across all events containing at minimum personal data, the event specific Data Processing Policies and the log showing when consent was given/withdrawn, as well as data which has been transmitted to third parties.

  - When the Contact Locator lists all possible names of attendees which satisfy the filter criteria, the data controller can simply navigate to the event of any of the attendees in the search result screen for further inspection.
  - The Contact Locator also features a tool to delete records across multiple events when consent is withdrawn.

- **Interactive Sites and Attendee App**

  Consent and Data Processing Policy text can easily be inserted into online Interactive Registration sites and the Attendee App, with the default text provided in the event setup. The Consent/Withdraw options are clearly shown, and no option will be ticked by default.

- **Handling of Cookies**

  Interactive EventsAIR registration sites require cookies for session handling only. EventsAIR cookies are safe because:

  - Cookies do not contain any personal data.
  - Cookies have the “Secure Flag” set.
  - Cookies expire after 3 hours.
  - Cookies are encrypted using strong ciphers/algorithms from the .Net Crypto libraries.

Physical Data Center Security

Azure is composed of a globally distributed datacenter infrastructure, supporting thousands of online services and spanning more than 100 highly secure facilities worldwide.

The infrastructure is designed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers. Azure has 52 regions worldwide, and is available in 140 countries.

A region is a set of datacenters that is interconnected via a massive and resilient network. The network includes content distribution, load balancing, redundancy, and encryption by default. With more global regions than any other cloud provider, Azure gives you the flexibility to deploy applications where you need them.

Azure regions are organized into geographies. An Azure geography ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.

Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies are fault-tolerant to withstand complete region failure, through their connection to the dedicated, high-capacity networking infrastructure.

Availability zones are physically separate locations within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Availability zones allow you to run mission-critical applications with high availability and low-latency replication.

Physical Security

Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data, and is committed to helping secure the datacenters that contain your data. We have an entire division at

Microsoft devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.

Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

- Access request and approval. You must request access prior to arriving at the datacenter. You're required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the datacenter required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire
- Facility's perimeter. When you arrive at a datacenter, you're required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team monitoring their videos at all times.
- Building entrance. The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter, and monitor the videos of cameras inside the datacenter at all times.
- Inside the building. After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacenter. If your identity is validated, you can enter only the portion of the datacenter that you have approved access to. You can stay there only for the duration of the time approved.
- Datacenter floor. You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacenter floor, you again must pass through full body metal detection screening. To leave the datacenter, you're required to pass through an additional security scan.

Microsoft requires visitors to surrender badges upon departure from any Microsoft facility.

Data Bearing Devices

Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped, we use a destruction process that destroys it and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. We determine the means of disposal according to the asset type. We retain records of the destruction.

Equipment Disposal

Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling and hardware disposal procedures to assure that hardware containing your data is not made available to untrusted parties. We use a secure erase approach for hard drives that support it. For hard drives that can't be wiped, we use a destruction process that destroys the drive and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. We determine the means of disposal according to the asset type. We retain records of the destruction. All Azure services use approved media storage and disposal management services.

Compliance

We design and manage the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. We also meet country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

For a full list of compliance standards that Azure adheres to, see the Compliance offerings.

Application Server Security Controls, Policies and Procedures

Overview

- The EventsAIR middle tier application Server is implemented as an Azure cloud service.
- While each tenant operates in a shared tenant environment, all tenant processes remain strictly private, as they do not share any data between them. Each tenant has a dedicated and fully isolated set of processes.

Application Server Security/Operational Controls

Web Application Firewall (WAF)

- EventsAIR is implemented with a WAF that protects against the top ten OWASP web threats such as SQL Injection, Cross Site Scripting and much more. Each client is protected by their own Web Application Firewall. The WAF logs are collected and saved in real time to the centralized OSSEC log server.
- Monitoring software inspects the logs in real time and will issue email alerts for specific WAF warnings.

Isolation in a Shared Tenant Environment

- The EventsAIR application server process operates in a shared tenant environment. However, each client process is isolated from another client's process, preventing accidental sharing of data.

Maximum Uptime

- Microsoft Azure and Centium Software provide SLA's stating a 99.95% uptime for all services.
- Each EventsAIR client process executes on two cloud server instances. Azure Load balancers direct the requests evenly between instances. To minimize downtime, only one instance at a time will be removed from the Azure Load balancer, to be updated, before the other instance is being updated.

Vulnerability Management

- EventsAIR is PCI compliant and adheres to a strict vulnerability management plan, to protect our Customers from the exploitation of information technology systems, from numerous external and internal sources.
- This includes automated patching as soon as a security threat is discovered. In order to eliminate downtime, each client process is executed on 2 instances. When one instance is patched, the other instance continues to work and vice versa.

- Microsoft is also one of the world's leading threat monitors. For more information, please visit https://msdn.microsoft.com/en-us/library/cc723507.aspx
- Patching details; Please refer to https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware
- Critical patching occurs within 48 hours, high patching occurs within 30 days, medium patching within occurs 60 days, and low patching occurs within 365 days.

Penetration Tests

- EventsAIR PCI DSS Level 1 compliance requires annual audits by an external, approved QSA. The penetration tests are conducted each year and form part of the ongoing compliance certification.
- Penetration tests are external, where the tester tries to compromise standard online registrations sites, or internal, where the tester simulates an attacker, who managed to log into a cloud service.
- PCI DSS compliance cannot be achieved, unless all medium or high-risk vulnerabilities are resolved and retested.
- In addition, Centium Software allows clients to conduct their own penetration testing at the clients cost. Once again, when these penetration tests find vulnerability issues of medium or high risk, Centium Software must rectify the issues and allow for retesting.
- As of March 2018, the PCI Security Standards Organization has added CDE perimeter testing at half between the annual audits.

  The scope of a penetration test, as defined in PCI DSS Requirement 11.3, must include the entire CDE perimeter and any critical systems that may impact the security of the CDE as well as the environment in scope for PCI DSS. This includes both the external perimeter (public-facing attack surfaces) and the internal perimeter of the CDE (LAN-LAN attack surfaces).

Encryption of Personal Data and Card Holder Data

- Data elements, which have been identified as personal, as well as data elements which contain card holder data, are encrypted, using modern .Net Crypto libraries and the AES 256 bit key length encryption algorithms.
- In addition, data at rest is encrypted using MS Azure TDE techniques.

Business Continuity

Microsoft Azure, in combination with Centium Software, provides a host of true business continuity features.

The building blocks of making business continuity a reality is Backup & Restore combined with Centium Software's continued deployment.

- **Backup – Restore** - In Azure, Geo Redundant Storage (GRS) such as blobs, tables, queues, and VM disks are all geo-replicated by default. GEO replication requires 2 or more data centers in a physical region, such as North America, Europe, and Australia. Physical data centers may be Amsterdam and Northern Ireland for Europe (Although more options are available), Australia East and Australia South East, US West Coast and US South East. (These are only some options.)

  In the event of a geo-failover, there will be no change to how the account is accessed (the URL and account key will not change). The storage account will, however, be in a different region after failover.

It is important to know where your data is geo-replicated, in order to know where to deploy the other instances of your data that require regional affinity with your storage. For more information see Azure Paired Regions. See https://docs.microsoft.com/en-us/azure/architecture/resiliency/recovery-loss-azure-region and https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions

ERT = Estimated Recovery Time, RPO = Recovery Point Objective

Automatic Backups: Full Backups are taken once a week, differential Backups twice a day and log Backups every 5 minutes.

A Retention time of 35 days allows to restore a database to a state every 5 minutes within the 35 days retention period.

In the event of a disaster, where the EventsAIR application server, as well as the database are no longer available for service, Centium Software will set up the Application server cloud service in a new geo region and provide a new copy of the database.

This means, that almost no data loss prior to the disaster occurred (potentially up to 5 minutes' worth of transactions may be missing) and no new transactions can be taken for the duration until the database and the application server are fully operational.

- **Live database replication** – The time to restore a database (in the point above,) is directly dependent on the size of the database. It is clear, that a 5GB database is much quicker to restore, then a 500 GB database. In order to avoid the potentially lengthy restore process, the customer may choose to replicate data to a database in a secondary data center.

  The time to restore is cut out of the process as the data is replicated in near real time. The restore process and therefore time to live is significantly reduced. This incurs a higher, monthly hosting fee as a second database in a second data center location needs to be maintained as an exact replica

Mobile Data

The security controls of our mobile apps (Organizer App and Attendee App) can be summarized as follows;

The app security is based on a large part on the security of the entire hosting platform. The app is a single device, which connects to the EventsAIR application servers. The phone does not hold any data, with the exception of data required for gamification such as picture upload, video streaming etc. All Event relevant data is stored in the events database.

This means, the data security is dependent on the hosting infrastructure security and the transmission between the phone and the host which is always encrypted and uses TLS 1.2.

The hosting platform is PCI DSS Level 1 compliant and certified, which requires an annual audit by a qualified, external PCI Auditor.

The data is transmitted from the mobile app to the EventsAIR database encrypted using https via TLS 1.2. EventsAIR Tenants are hosted on a shared server with other tenants however, data is not shared because each tenant on the server has a dedicated server process with its own memory space. Finally the data is stored in the EventsAIR database, which is not shared but dedicated.

Storage of the data occurs in the region or economic are, our clients are based in. Current regions are Australia, South East Asia, Asia, Middle East, Europe, North Amerika (US and Canada), and South America.

The database as well as the backup database are encrypted using Microsoft TDE (Transparent Data Encryption). This applies to the entire database. Were a malicious person to get somehow hold of the database, it would be of no use, since not a single data element is in clear text.

Every alteration to code or new code is subject to peer review and sign off before it even enters the QA process. We also adhere to secure coding practices and OWASP top 10.

Application Server Policies and Procedures

Continuous Deployment Process

EventsAIR uses a continuous deployment model that offers distinct possibilities in regard to business continuity and downtime.

For instance, if a primary datacenter experienced a disaster, the automated GEO backup located in the paired data center would be accessed and restored to its operational functionality within one hour.

The following automated processes drive continuous deployment:

- The Centium Software developed ConfigManager, in conjunction with TeamCity and Octopus deployment controllers, are tightly integrated with the MS Azure API. It is the main tool, which allows Centium Software staff to commission a new client in a consistent, automated manner, without any further human assistance.
- Unique, auto generated sets of credentials are used for each customer.
- During the commissioning of a new cloud service, the following actions are taken:
  - The cloud service page file size is set.
  - Apply the baseline GPO (Group Policy Object) Pack built using Security Compliance Manager for Server 2016. This includes disabling weak Ciphers, enabling TLS 1.2 or higher, applying setting for inbound/outbound firewall ports.
  - Deal with Registry Changes that require reboots.
  - Ensure that TSL 1.0/1.1 are disabled.
  - Disable browsers on the cloud service, flagging a reboot is needed.

Vulnerability Management Policy and Procedure

Security patch management (patch management) has become a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. Consequently, all IT resources must be securely hardened and configured with all necessary and appropriate patches and system updates in order to prevent the exploitation or disruption of mission-critical services.

In accordance with best practices for security patch management, the subsequent three (3) security concerns will be highlighted throughout the Security Patch Management policy. They are as follows

- **Vulnerabilities**: Software flaws or a misconfiguration that may potentially result in a weakness in the security of a system within the system components directly associated with the customer data environment or any other IT resources
- **Remediation**: The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of affected software.

- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses and Trojan horses.

  Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments directly associated with the customer environment. This includes but is not limited to the following:

  - Network devices and all supporting hardware and protocols.
  - Operating systems within the development and production environments.
  - Applications within the development and production environments.
  - Any other mission-critical resources such as the customer data environment that require patches and security updates for daily operations.

Centium Software Configuration/Deployment Standards for New Vulnerabilities

When any new vulnerabilities are discovered, the impact of these vulnerabilities will be determined. If there would be an impact on the security of the EventsAIR systems, Centium Software's configuration and deployment standards will be updated to address the vulnerability. Proper change management procedures are followed.

Additionally, the MS Azure Security Patch Management Program (SPMP) is implemented, which consists of the following initiatives:

- A formalized Security Patch Management Program employee, complete with his/her roles and responsibilities.
- Comprehensive inventory of all system components directly associated with the customer environment.
- Comprehensive inventory of all other IT resources within the EventsAIR hosting sites not directly associated with the customer environment.
- Subscription to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues.
- Procedures for establishing a risk ranking regarding security patch management. This includes but is not limited to:
  1. the significance of the threat,
  2. the existence and overall threat of the exploitation and,
  3. the risks involved in applying security patch management procedures (its effect on other systems, resources available and resource constraints).
- A database of remediation activities that need to be applied.
- Test procedures for testing patches regarding remediation.
- Procedures for the deployment, distribution and implementation of patches and other related security-hardening procedures.
- Procedures for verifying successful implementation of patches and other related security-hardening procedures.
- Installation of applicable critical vendor-supplied security patches within one month of release.

- Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

System Components and Asset Management

Centium Software maintains a list of all system components. Changes to the list is subject to approval and documentation, specifically opening of new ports, changes to the WAF configuration, inclusion of third party software, changes to the Azure Firewall and more.

MS Azure maintains a metering platform for billing purposes. Every asset is listed, usage documented and cost assigned. This is the most accurate asset management which can be reported on.

Procedures to Protect Client Cloud Services Against Emerging Malware/Virus Threats

Microsoft is one of the leading threat monitors worldwide and responsible for:

- Proactively deploying anti-malware and anti-virus software on our clients EventsAIR cloud service.
- Ensuring that anti-virus programs are capable of detecting, removing and protecting against all known types of malicious software.
- Generating and storing audit logs from scans in a centralized logging server.
- Ensuring that anti-malware/anti-virus is always up to date and can't be switched off.
- Ensuring that all operational procedures for protecting systems against malware are documented, in use and known to all affected parties.

Centium Software established a process to identify security vulnerabilities:

- Centium Software performs monthly vulnerability tests to identify whether all system components continue to be protected. The tests are conducted by an external Service Company called "Comodo".
- Centium Software/Comodo assigns risk rankings (high, medium, low) to all identified vulnerabilities.
- Microsoft Azure immediately installs critical security patches if/when required. The clients don't experience any downtime.

Maintain a Risk Assessment Matrix

The Risk Assessment report is reviewed, at minimum, on an annual basis. Changes to critical system components will trigger a new assessment report.

Risks are graded as low, medium and high.

		Consequence		
		Minor Impact	***Moderate Impact***	***Major Impact***
Likelihood	***Very likely***	Medium Risk	High Risk	High Risk
	Likely	Medium Risk	Medium Risk	High Risk
	Possible	Low Risk	Medium Risk	High Risk
	Unlikely	Low Risk	Low Risk	Medium Risk

Risk categories that are assessed include system components, vulnerability threats and human threats

Incident Response Plan Policy and Procedure

Centium will ensure the Incident Response Plan adheres to the following conditions for the purposes of complying with the PCI DSS initiatives and extends this plan to GDPR:

- The scope of the Incident Response plan covers all security (beyond just payment card industry related) incidents as well as all privacy breach incidents (GDPR)
- The Incident Response plan includes, at a minimum, roles, responsibilities and communication strategies in the event of a compromise, including, also at a minimum, notification of the payment brands or assisting the data controllers to notify the Supervisory Authorities of their countries.
- The Incident Response plan includes a specific incident response, business recovery and continuity procedures and data backup processes.
- The Incident Response plan includes legal requirements for reporting any compromises to the data subject's personal data.
- The Incident Response plan includes coverage and response mechanisms for all critical system components and all other IT resources deemed critical by Centium Software.
- The Incident Response plan also includes reference or inclusion of incident response procedures from the payment brands.
- The Incident Response Plan is to be reviewed annually.
- Designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical Intrusion Detection Systems (IDS) alerts and/or reports of unauthorized critical system or content file changes.
- Commitment to affected Customers; The customer will be asked to provide contact details to a designated incident contact email, SMS or phone. This line must be contactable 24/7. Typically these are contact details of IT security, IT Incident Response team, Data Protection officer or other. Centium will contact the designated incident contact within 8 hours of becoming aware of an incident having occurred.
- Staff with responsibilities for security breach responses is at minimum trained annually.
- Monitoring and responding to alerts from security systems, including detection of unauthorized wireless access points, constitute an important component of the Incident Response plan.
- Processes are in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments as needed.

Standard Operating Procedure (SOP) Incident - Response

- For any incident that has been detected, the Incident Response Team is to be immediately notified.
- The Incident Response Team is to formally assume control and to identify the threat and its severity to the organization's information systems.
- If the incident encompasses a complete data center failure, and it is established that the outage can't be tolerated by the client, the Disaster Recovery plan is executed.
- In identifying the threat, the Incident Response Team is to specifically identify which resources, both internal and external, are at risk and which harmful processes are currently running on resources that have been identified as at risk.

- The Incident Response Team is to determine whether the resources at risk (hardware, software, etc.) require physical or logical removal. Resources posing a significant threat to the continuity of the business are to be immediately removed or isolated, either physically or logically. Resources that may require physical or logical removal or isolation may include, but are not limited to, the following:
    - The affected client's cloud service implementation or, Potentially an entire cloud server (2 instances)
    - The affected client's database or, potentially the entire database Server
    - The Vault Service
    - Blob Storage
    - Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) (WAF)
    - Remote access (Shutting down/isolating affected RDP gateways to the Cloud Services)
- If the incident has affected the customer data environment (i.e. in cases where the evidence shows that custom, marketing or notes fields, which have been tagged as personal data, have been breached), the data processor (Centium Software) must notify the data controller (EventsAIR customer) as soon as practical and ensure, that the data controller notifies the Supervisory GDPR Commission in their country within 72 hours.
- If the incident has in any way resulted in a criminal matter that may be readily identified, Centium Software must immediately report it to law enforcement officials and Supervisory GDPR Commission's (via Data Controller)
    - Legal Preparation and Log preservation. Preserve all customer logs from just before the incident, to after the incident, including SEQ, IIS, OSSEC, WAF, SNORT, Database.
- Investigating the incident is also a critical process within the Incident Response plan. Proper investigative techniques are to include, but are not limited to, the following:
    - Understanding how the incident occurred and what led to the compromise.
    - Reviewing all necessary system documentation such as logs, audit trails, rule sets, configuration and hardening standards and all other supporting documentation.
    - Interviewing personnel as needed.
    - Examining any third-party providers and their respective products and services that are utilized within Centium Softwares' network architecture.
    - If warranted, a third-party resource for assisting in the investigation of the incident may be utilized (this will be done at the management's discretion).

Recovery from an Incident

Recovery procedures will include but are not limited to the following:

- Restoring systems from clean backups (a trusted source only, before incident occurred).
- Completely rebuilding systems as needed and warranted.
- Replacing systems as needed (this includes all system components within the customer data environment and any other IT resources deemed critical by Centium Software).
- Reconfiguring network security (stronger, more adaptive configuration and hardening rules) for all system components within the customer data environment and any other IT resources deemed critical by Centium Software.

Post-Incident Activities and Awareness

A formal and documented Incident Response Report (IRR) is to be compiled and given to management of Centium Software within an acceptable timeframe following the incident. The IRR must contain the following elements:

- Detailed description of the incident in the internal Centium Software Wiki.
- Response mechanisms undertaken.
- Reporting activities to all relevant third parties as needed.
- Recovery activities undertaken for restoring affected systems.
- A list of Lessons Learned from the incident and which initiative Centium Software can take to mitigate and hopefully eliminate the likelihood of future incidents.
- In some cases Legal Preparation (Including pre-incident database restore, post incident database capture, securing of all Logs during the time of the incident including SEQ, OSSEC, DATABASE, IIS, WAF, Event Logs).

Business Continuity and Disaster Recovery

The assumption is that a client installation in a data center is completely offline. Both, the application server and the SQL Azure database are offline as a result.

We also assume that the client didn't make use of geo replication. In other words, there is no second database to which failover could occur and the database is operational after that.

Business continuity can then be defined as the restoration of the database and the application service to resume full operational activity. These steps are:

1. Verify how many clients are down.
2. Decide in which data center Azure stores the geo-backup of the affected client(s).
3. Restore the database(s) in that location.
4. Deploy the client(s) as new client(s) in the same data center.
5. Execute scripts to fill blob storage.
6. Establish communication throughout the process, according to the incident response plan.

The longest process is the restore of the database(s), dependent on the size of the respective database(s). The expected data loss is at most 5 minutes from the time the last transaction log backup (every 5 minutes) was taken and the loss of the data center.

MS Azure SQL Server Security Controls, Policies and Procedures

Overview

The MS Azure SQL Service is a cloud service. Each client is serviced by a dedicated, not shared, database.

Centium Software developers build applications on top of large scale data-tiers consisting of multiple database servers. A standard application pattern is to provision a single database for each customer.

MS Azure SQL Server Security Controls

Access to database via a DB Connection String

For clients, who wish to use their own reporting services, we have the ability to provide a **read-only** SQL Azure Connection String.

By default, Azure locks down the ports so that no IP address can access the database server. To enable additional security, the IP address or addresses, from which the external reports are executed, must be whitelisted in the MS SQL Azure firewall.

EventsAIR Application Server

Except for providing a SQL Azure connection string to our clients, the only other way of accessing the database is via the EventsAIR Application Server.

Centium Software use MS Azure Network segregation which results in distinct logical networks. Each logical network is protected by an Azure firewall. All cloud services are additionally protected by the WAF.

Transparent Data Encryption (TDE)

All databases are encrypted on disk, using MS TDE as the encryption of choice. This means that all database backups are also encrypted.

The protection extends to all data elements in the database, be it personal data or credit card data (if stored in the Credit Card Vault).

Deployment of Database

During the implementation of a new client, the new client database password is generated uniquely for each client. No two clients, share the same application server access password.

The passwords are unknown to most of the internal support, IT and development staff.

EventsAIR SQL Azure Policies and Procedures

Pro-Active Monitoring of Database Performance and Size

Centium Software IT staff monitor the database performance levels close to 24/7, supported by staff in the US, UK and Australian offices.

StatusCake is used to ping all EventsAIR customers online sites. The ping tests services in the application server, as well as connectivity to the database.

In addition, an internal ping is executed once a minute and covers all online sites on the cloud server. The logs from the ping are exported, in real time, to the central log server from OSSEC and notification outage emails are sent to relevant monitoring mail boxes.

MS SQL Credit Card Vault Security Controls, Policies and Procedures

Overview

NOTE: Credit Card Details taken within the standard registration process. When an attendee selects any registration category, function or accommodations, are **not** stored in the credit card vault. The credit card details are discarded, as soon as a registration has completed.

Customers may have a business need to securely store credit card data for a period of time (e.g. Hotel booking guarantee). EventsAIR offers a Credit Card Vault infrastructure which consists of 2 logical network segments, separated by Azure firewalls.

1. Vault application Server
2. Vault Azure Database

Vault Security Controls

- **Web Application Firewall**

  The Vault Application Server can only be reached by the EventsAIR Application Server on port 443. It is protected by a WAF which is configured to not only alert in the event of top ten OWASP web threats such as SQL Injection, Cross Site Scripting and much more, but many other online threats. The WAF logs are collected and saved in real time to the centralized OSSEC log server.

  Monitoring software inspects the logs in real time and will issue email alerts for specific WAF warnings.

- **2048 Bit Key Length RSA Public/Private Encryption**

  The card holder data has already been encrypted by the application server, using AES 256 bit key length. Before writing the data to the vault, the vault application server encrypts the card holder data a second time using a public/private RSA key pair with 2048 byte key length.

- **Removal of Card Holder Data After the Event**

  Card Holder data is automatically removed after the event closure date plus a configurable number of days after the event.

  This service runs as a process on the Vault database.

- **Annual Vault Public Key Rotation Facility**

  The key rotation utility will use the old key and generate a new key.

  The utility rotates through all card holder records, decrypts using the old key and re-encrypts, using the new key.

Vault Policies and Procedures

- **Key Custodians and Key Rotation Process**
  - Only store sensitive data which is needed to support the business.
  - Use strong approved algorithms (AES, RSA public key cryptography, and SHA-256 or better for hashing).
  - Use strong random numbers (Ensure that random algorithms are seeded with sufficient entropy).
  - Ensure that the cryptographic protection remains secure even if access controls fail (encrypted in DB).
  - Ensure that any secret key is protected from unauthorized access.
  - Cycle the encryption key at least once a year or upon leaving of a key employee (PCI DSS).
  - Store unencrypted keys away from the encrypted data.

- Separation of keys (Split knowledge and establishment of dual control of cryptographic keys).
- Protect keys in a windows key store or encrypt relevant sections in a config file.
- Document concrete procedures for managing keys throughout the lifecycle.
- Change Keys regularly and sign off on key change.
- Document concrete procedures to handle a key compromise (see Req 3-6 Key Management Policy and Procedures.docx).
- Render PAN (Primary Account Number), at minimum, unreadable anywhere it is stored.
- Protect any keys used to secure cardholder data against disclosure and misuse.

Safe Data Destruction when leaving EventsAIR

When leaving EventsAIR, a data retention period of 90 days follows, to allow for the extraction of required data.

Centium Software will provide ongoing notices during this period so that the client has sufficient time, until the data is permanently purged.

The device data cleansing is performed in accordance with the NIST (National Institute for Standards and Technology USA) 800-88. For more reading, please refer to https://www.microsoft.com/en-us/trustcenter/privacy/you-own-your-data