Security Statement

Last Updated: July 5th, 2018

Introduction

eSpatial Solutions Ltd. (referred to as eSpatial for the remainder of this document) is committed to protecting and securing the data it accesses, stores and processes from its customers. eSpatial maintains appropriate administrative, technical and physical procedures to safeguard and secure Customer Data. eSpatial is aware of laws and best practices governing Customer Data and implements effective controls to ensure appropriate processing and protection.

The data security controls described in this document are in place at eSpatial to help ensure that Customer Data is appropriately protected.

Customer Data provided to eSpatial is considered Highly Confidential Information and is afforded the highest level of security at the company.

Policies and Procedures

eSpatial has documented and implemented policies and procedures that regulate the processing of Customer Data, including its receipt, transmission, storage, distribution, access and deletion. eSpatial policies and procedures are designed to comply with all applicable laws, rules and regulations in the countries in which it conducts business.

eSpatial maintains a comprehensive set of information security Policies and Procedures that are approved by Senior Management and are reviewed and updated regularly to remain compliant with the law and current industry practices. These Policies and Procedures include:

- Organizational Security
- Physical and Environmental Security
- Communications and Connectivity
- Change Control
- Data Integrity
- Incident Response
- Privacy
- Backup and Offsite Storage

- Vulnerability Monitoring
- Information Classification
- Data-handling
- Security configuration standards for networks, operating systems, applications and desktops

Physical SaaS Production Environment

eSpatial employs a public cloud deployment model using both physical and virtualized resources for its software-as-a-service ("SaaS") solution (eSpatial). All software maintenance and configuration activities are conducted by eSpatial employees remotely from our corporate office. Our provider of choice for the public cloud is Amazon Web Services (AWS). Detailed information on AWS compliance, certifications and security can be found at the following URL https://aws.amazon.com/compliance/.

eSpatial is a multi-tenant solution and logical access controls using authentication and roles ensure the necessary separation between data from different clients. All infrastructure responsibilities lie with eSpatial, and clients are provided with functionality to manage their own users and roles at the application level.

eSpatial is ISO 27001:2013 certified (our certificate is available here) which ensures that we have a world class framework on which to base our information security and are regularly audited by an external third party to manage and maintain our security certification. This combined with our many years of experience in operating highly secure SaaS solutions means that your data is secured to the highest standards. eSpatial employs industry standard practices for security controls such as firewalls, intrusion detection, change management complete with written security policies that are regularly reviewed.

Scalability

eSpatial's distributed architecture for data collection and processing allows it to scale horizontally as the number of clients and volume of traffic increase. eSpatial uses multiple monitoring processes and tools to continuously track network resources, operating systems, applications and capacity. Systems are scaled up when predetermined capacity thresholds are reached.

SaaS Management

The eSpatial Cloud Operations team is responsible for all aspects of the production environment. The Cloud Operations team is set up separately and independently from the corporate network IT organization to ensure the necessary separation of duties. Cloud Operations' professional depth enables eSpatial to provide SaaS services at the highest levels of efficiency.

Risk Management

eSpatial has practices in place, as part of its business continuity planning, to assist management in identifying and managing risks that could affect the organization's ability to provide reliable services to its clients. These practices are used to:

- identify significant risks for the organization
- initiate the identification and/or implementation of appropriate risk mitigation measures
- Assist management in monitoring risk and remediation activities.

Controls

Physical Access Control

Physical access to facilities where data is processed is restricted through use of access control procedures for authorized users (e.g. badge access, reception at entrance, etc.). Visitor access must be logged in an access log and visitors are escorted through restricted areas in the facility.

Asset addition / removal processes from the facility are documented.

Intrusion detection alarms are installed at egress and ingress points and monitored.

Clean desk / clear screen policy is defined.

Logical Access Control

eSpatial ensures authentication and authorization controls are appropriately robust for the risk to the data, application and platform.

eSpatial monitors access rights to ensure access adheres to the least privilege principle commensurate with the user's responsibilities. eSpatial logs all access and security events, and uses software that enables rapid analysis of user activities.

Logical Access Control Policy

Logical access control policy and corresponding procedures are documented. The logical access procedures define the request, approval, access provisioning and de-provisioning processes. The logical access processes restrict user access (local and remote) based on user job function for applications, databases and systems (role / profile based access) to ensure segregation of duties.

User access reviews are performed periodically for each application, database or system housing computer data (e.g. quarterly, semi-annually or annually) to confirm access and privileges are appropriate.

Procedures are documented for users who have joined, left or changed roles within the company.

Platform / Operating System Level ID Administration

The process for management of privileged user accounts is defined. A review process is in place and privileged accounts are reviewed periodically (quarterly) to ensure access is restricted, appropriate and documented (requests and approvals) prior to account creation.

Remote control of desktop is restricted to a specific role (e.g. helpdesk admin) and remote control is not permitted unless and until the end user gives permission.

Authentication and Authorization

Documented password policy covers all applicable systems, applications and databases. Password best practices are deployed to protect against unauthorized use of passwords.

Password policy includes the following components:

- Password is communicated separately from User ID
- Password is not shared
- Initial password generated is random
- Forced initial password change
- Minimum password length
- Password complexity
- Password history

Passwords are saved only as one way hashed / encrypted files. Access to password files is restricted only to system administrators.

If the authentication engine for application fails, the default action is always to deny access.

Data Access Control

An Authorization Concept for user and administration rights is designed to ensure that access to the data in the system is enabled only to the extent required for the user to complete the relevant task according to the user's internal task distribution and separation of functions. Rules and procedures for creating, changing, and deleting authorization profiles and user roles in compliance with data protection rules are described therein. The Authorization Concept must show which job holder may carry out administrative tasks (system, User, operation and transport) and which user groups may perform which activities in the system. Responsibilities are regulated and segregation of duties exists.

Each access authorization is linked to a data access authorization, by linking it to one or more roles defined in the Authorization Concept. With the applications and within these applications, each access-authorized person may access only the data that he specifically needs to process the current transaction, according to the order and which access is configured in his individual authorization profile.

To the extent that data of multiple customers is stored in the same database or is processed with the same data processing system, logical access restrictions are provided which aim exclusively at processing the data for the customer concerned (multi-tenancy). The data processing function itself is limited to the extent that the minimum functions required will be used to process the personal data.

The scope of the authorizations is limited to the minimum needed to perform the authorized person's duties and functions. To the extent that certain functions can be limited in time without lowering the data processing quality, authorization time is limited to access personal data, as certain systems have automatic expiration times (e.g. Active Directory)

A process for requesting, approving, assigning, revoking and checking data access authorizations is set up, described and used on a mandatory basis. Rules and procedures for granting / revoking authorizations or assigning user roles are described in the relevant policies.

Authorizations must be linked to a personal user ID and an account. No group accounts / passwords can be used by multiple people.

When granting authorizations or assigning user roles, only the number of data access rights needed for performing the person's duties are assigned (need-to-know principle).

If an individual leaves the company or moves to a different department, all data access rights for all data processing systems and data storage areas that are no longer necessary for the performance of that person's duties are revoked. Steps are taken to ensure that all parties involved are notified of the fact that employees have left the company or changed roles (in particular IT administrators)

Communication and Connectivity

eSpatial utilizes various methods of communication, including email and the corporate intranet to update employees on current events and policies. Information relevant to employees is shared, such as corporate data, industry news, training and development materials, employee resources, and other corporate policies. Cloud Operations has a dedicated intranet section to publish information relevant to Cloud Operations staff, such as technical materials, policies and procedures.

Updates to key documents, such as policies, requires email notification to the affected staff.

eSpatial implements robust controls over its communication network to safeguard data, tightly controls access to network devices through management approval and subsequent audits, disables remote communications if no business need exists, logs and monitors remote access devices, and uses strong authentication and encryption to secure communications.

Network identification

Network diagrams highlighting key internal network components and Demilitarized Zones (DMZ) are documented.

Data flow is documented for all Customer Data, from the Customer environment to eSpatial end-point.

Firewall management processes are documented. All changes to the firewall are performed via change management processes. Firewall access is restricted to a small set of administrators with appropriate approvals.

Periodic network vulnerability scans are performed and any critical vulnerability identified is promptly remediated.

Network Security Policy

Defined Access Control Lists (ACLs) to restrict traffic on routers and / or firewalls are reviewed and approved by network administrators. IP addresses in the ACLs are specific and anonymous connections are not allowed (except ports 443 and port 80 on the web applications)

Periodic recertification and authorization of firewall rules are performed.

Remote Access Administration

Remote Access Settings:

- Unauthorized remote connections from devices (e.g. modems) are disabled as part of standard configuration.
- The data flow in the remote connection is encrypted using a static key and TLS.

Email and IM

Policies and procedures are established and adhered to for proper control of electronic mail and/or instant messaging system that displays and/or contains Customer Data.

Authorized E-Mail Systems

Preventative and detective controls block malicious e-mails and attachments.

Data Integrity

eSpatial Policies and Procedures are designed to ensure that any data stored, received, controlled or otherwise accessed is not compromised and remains intact.

Data Transmission Controls

Data transmission control processes and procedures are in place to ensure data integrity is documented.

eSpatial uses SSL, which encrypts data that is transmitted to our web application with the highest levels of encryption available.

Data Entry Control

Vulnerability Monitoring

eSpatial continuously gathers and analyses information regarding new and existing threats and vulnerabilities, actual attacks on the company or others, and the effectiveness of the existing security controls. Monitoring controls include related policy and procedure, virus and malicious code, intrusion detection, and event and state monitoring. Related logging process provides an effective control to highlight and investigate security events.

Vulnerability Policy and Procedure

Penetration testing of the SaaS application is performed annually. The tests are always performed externally by a reputed external organization. All issues rated as high risk are remediated within appropriate timelines.

Anti-virus and Malicious Code

Servers, workstations and internet gateway devices are updated periodically with latest antivirus definitions. Defined procedure highlights all anti-virus updates. Anti-virus tools are configured to run scans, virus detection, real time file write activity and signature file updates. Laptop and remote users are covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (e.g. freeware) applications are documented.

Alert events include the following attributes:

- Unique identifier
- Date
- Time
- Priority
- Source IP address
- Destination IP address
- Event Description
- Notification sent to security team
- Event Status

Security Event Monitoring

Security events are logged (log files), monitored (appropriate individuals and automated checks) and addressed. Network components, workstations, applications and any monitoring tools are enabled to

monitor user activity. Organizational responsibilities for responding to events are defined. Configuration checking tools are utilized that record critical system configuration changes and administrators are alerted at the time of change. Retention schedule for the various logs are defined and adhered to.

Incident Response

eSpatial documents a plan and associated procedures in case of an information security incident. The Incident Response Plan clearly articulates the responsibilities of personnel and identifies relevant parties for notification. Incident response personnel are trained, and execution of the incident response plan is tested periodically.

Incident Response Process

Information security incident management and policy procedures are documented. The incident management policy and/or procedures include the following attributes:

- Organization Structure is Defined
- Response Team is indentified
- Response team availability is documented
- Timelines for incident detection and disclosure are documented
- The process for the incident response lifecycle is defined and includes the following steps:
    - Identification
    - Incident Severity classification
    - All communication documentation
    - Final resolution
    - Training of personnel
    - Testing to ensure remediation is effective
    - Reporting of the incident
    - Customer notification.

Escalation / Notification

The incident response process is executed as soon as eSpatial become aware of an incident.

Control of Processing Instructions

Employee Education and Awareness

eSpatial employees are required to be familiar with the protection of Customer Data. Methods of awareness include:

- In-person and on-line information
- E-mail from IT to employees
- Internal web portal

Availability Control

Backup and Offsite Storage

eSpatial has a backup policy and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data (onsite and off-site). eSpatial also ensures that Customer Data is securely transferred or transported to and from backup locations. eSpatial also conducts periodic tests to ensure that data can be safely recovered from backup devices.

Backup Process

Backup and offsite storage procedures are documented. Procedures include the ability to restore applications and operating systems.

Backup Media Destruction

Procedures are defined for instructing personnel on the proper methods of backup media destruction. Backup media destruction by a third party is accompanied by documented procedures for destruction confirmation.

Offsite Storage

Physical security for the offsite facility is documented. Access control is enforced at entry points and in storage rooms. Access to the offsite facility is restricted and there is an approval process to obtain access. Backup storage devices (e.g. backup tapes) are encrypted as applicable. Secure transportation procedures (e.g. inventory tracking, signed checklists) or media to and from the off-site location are defined.

Separation Control

Organizational Control

Operations

eSpatial has documented IT operational procedures to ensure correct and secure operation of its IT assets.

Operational Procedures and Responsibilities

Operational Procedures are documented and successfully executed. The documentation includes the following components:

- Scheduling requirements
- Maintenance and troubleshooting of systems
- Documented procedures and the reporting structure for escalations.

Problem Remediation Management

Problem remediation management process and procedures are documented. The problem management lifecycle includes the following steps:

- Problem identification
- Assignment of severity to each problem
- Communication
- Resolution
- Training (if required)
- Testing / validation
- Reporting

End of Life and Faulty Equipment

Procedures exist for the disposal / reuse of retired or failed equipment including proper removal of Customer Data. Notification of any misplaced assets is made to eSpatial Management in all cases.

Change Management

Changes to systems, network, applications, and data file structures or other system components and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.

Change Policy Procedure

Change management policy includes application, operating system and network infrastructure, including firewall changes. Emergency change management procedures are specified, including factors leading to an emergency change.

The procedure includes the following attributes:

- Clearly defined roles and responsibilities
- Impact or risk assessment of the change request
- Backout or recovery plans
- Testing prior to the implementation of the change
- Security implications
- Authorization and Approval (This does NOT include customer approval for the SaaS environment)
- Post-installation sign-off
- Post-change review and notification

Emergency Fix Procedures

Emergency change procedures have stated roles and responsibilities for request and approval. The procedures include a post-change implementation validation. The procedures include post-emergency change documentation update.

Data Privacy

Web Application Configuration

Multi-tiered architecture is established where the web presentation, business logic and data tiers are separated into separate servers and firewall zones.

Periodic penetration testing is performed against the application website and includes the following attributes:

- Authentication bypass
- Injection
- Broken authentication and Session Management
- Cross site Scripting
- Insecure Direct Object References
- Security misconfiguration
- Sensitive data exposed
- Missing function Level Access Control
- Cross Site Request Forgery (CSRF)
- Known vulnerable Components

- Unvalidated Redirects and Forwards
- Account traversal
- Privilege Escalation
- Data extraction

Monitoring tools are in place to monitor website uptime and to alerts when issues arise. Restrictions are placed on web server resources to limit denial of service (DoS) attacks.

System / Software Development

eSpatial has an established software development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing and implementing our products.

Development Lifecycle

eSpatial's Software Development Life Cycle methodology includes version control and release management procedures. System documentation is managed by appropriate access controls. Software vulnerability testing is completed and any vulnerability gaps identified are remediated in a timely manner.

Security in Development and Support Process

eSpatial follows the Waterfall development methodology in which products are deployed following comprehensive requirement gathering, system design, implementation, testing and deployment phases. Security and security testing are implemented throughout the entire software development methodology.

Quality Assurance is involved in the lifecycle and security best practices are a mandated aspect of all development activities. Our main test areas include volume, stress, security, performance, resource usage, configuration, compatibility, installation, and recovery testing.

The development process includes a review of all embedded third party components to ensure that security updates are incorporated. Use of open source software is subject to technical review and approval.

Standard Builds

Information systems are deployed with appropriate security configurations and are reviewed periodically for compliance with eSpatial security policies and standards.

Secure Configuration Availability

Standard security hardening procedures include:

- Security patches
- Vulnerability management
- Access, rights and permissions.

System Patches

Security patch process and procedures, including patch prioritization are documented.

Vulnerability Analysis

Periodic penetration testing of the external perimeter is performed regularly using tools for checking, monitoring and auditing of the environment.

Operating System

Documented operating system versions are implemented for our SaaS environment. Standard Security is implemented on all the operating systems and versions.

Human Resources Security

Employee Screening

Confidentiality and security is a serious concern for our clients and eSpatial employees are required to undergo background checks before being employed.

Terms of Employment

General information security responsibilities are documented in eSpatial's New Employee Handbook, which all employees must sign when joining the company.
Specific security responsibilities are documented in job descriptions for Cloud Operations team staff with security duties.

Training

General information security training is provided to all new employees (both full time and temporary) when they join. A compulsory annual security and privacy training requirement ensures employees refresh their knowledge and understanding.

Development and Cloud Operations staff receive further training specific to product development, deployment and management of secure applications. Additional security training is also provided to employees who handle client data.

Termination of Employment

eSpatial's Human Resources department manages a formal termination process, which includes notification of Corporate IT, Cloud Operations and Facilities, return of assets and access cards. The exit interview reminds ex-employees of their remaining employment restriction and contractual obligations.

Confidentiality and Non-Disclosure Agreements

All employees must sign eSpatial's confidentiality agreement (NDA) at the time they join the organization. Periodic verbal and email reminders are provided. Upon termination, employees are provided another copy of their agreement.

Supplier Relationships

eSpatial may use contractors for development and testing tasks. These individuals work under the direct supervision of eSpatial employees and may have access to client data in accordance with contract terms.

eSpatial does not give suppliers direct access to client data or network/equipment management responsibility. They do not have direct access to client data or the eSpatial SaaS network environment.

eSpatial uses exclusively world renown third party suppliers with stellar background, such as Amazon (for cloud infrastructure), and google.