Data Privacy and Security Policy

This document contains proprietary and confidential information pertaining to Zetta Systems and should not be used, reproduced, or disseminated without the prior written approval of Zetta Systems Any unauthorized use, reproduction or dissemination of this document and any content hereof constitutes infringement of trade secrets and will result in serious legal liabilities.

Table of Contents

About this Document

Document Owner:
Kaloian Parchev

Document Supervisor:
Petar Petrov

Release Date:
Dec-2015

Revision Date:
Dec-2022, v9

1. General Information

1.1. Scope

This policy applies to Zetta Systems, its IT infrastructure, employees, third party contractors or any other propriety of Zetta Systems.

1.2. Purpose

Zetta Systems maintains a set of information security policies and procedures that are approved by senior management and are reviewed and updated to remain aligned with the law and current industry practices or frameworks.

2. Revision policy

This policy is revised every **six (6)** months by the person acting as **Chief Technology Officer** and Zetta Systems' **management.**

3. Law Enforcement

3.1. General Data Protection Regulation (EU) 2016/679 ("GDPR")

Zetta Systems does not process personal data as part of its commercial activities. Subjects whose data is being collected should be given notice of such collection.

3.2. Rights when collecting, processing, or storing your personal data

- **Purpose:**
  data collected should be used only for stated purpose(s) and for no other purposes.
- **Consent:**
  personal data should not be disclosed or shared with third parties without consent from its subject(s).
- **Security**
  once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- **Disclosure:**
  subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- **Access:**
  subjects should grant access to their personal data and allowed to correct any inaccuracies.
- **Accountability:**
  subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.
- **Removal:**
  subjects must be able to remove their personal data upon request.

4. Public services

4.1. Website

4.1.1. TBD

4.2. E-mail provider

4.2.1. TBD

5. Data Management

5.1. Data encryption

5.1.1. Zetta Systems is encrypting any sensitive information or data as follows:
5.1.2. Data encryption-at-rest.: **AES256**
5.1.3. Data encryption-in-transit: **SSL/TLS**
5.1.4. Backup and archiving data use **AES256**

5.2. Device Encryption

Data encryption applies for all company desktop, portable and mobile devices. The following rules are implemented:

5.2.1. Any data at rest stored on the employee's systems is protected by **Microsoft Bit-Locker.**
5.2.2. Any confidential data is encrypted at least with **Microsoft EFS.**
5.2.3. Access and rights to the recovery certificate(s) are managed by Zetta Systems' **Chief Technology Officer.**

5.3. Data Control

5.3.1. Zetta Systems does not store, transfer, manipulate or process any customer data outside of the client's infrastructure, except when this is required by the client or both parties have contract agreement describing what is allowed and what is not.
5.3.2. Storing customer or personal data depends on 3. Law Enforcement and 4.3 Data Control. Customers may request their data deletions when:
5.3.2.1. They need to remove their personal data from Zetta Systems upon contract termination or any other reason covered by the General Data Protection Regulation **(EU) 2016/679**
5.3.2.2. The customer requires to remove their data due to security concerns
5.3.2.3. Legal purposes, requested by the client.

5.4. Hard-copy media

5.4.1. All confidential information in hard-copy form is stored in locked cabinets within the Zetta Systems office where it is created or received.
5.4.2. All Zetta Systems' offices are located in secure buildings and are locked during non-business hours.
5.4.3. Only those individuals who have a need to know have access to confidential information.

5.4.4. Documents that contain confidential information, and are marked as such, are never left unattended in an empty office. If such documents must be transported to another location, the individual who transports the documents ensures that the document is under his/her control at all times and is returned to its locked file cabinet.

5.4.5. Any copies of all or a portion of any confidential document are marked as 'Confidential' and treated in the same manner as the original.

5.5. Media Sanitization

Zetta Systems has a strong policy for the media life cycle management and destruction of any non-operational **data storage media (soft copy)**.

5.5.1. **Data storage media** destruction is handled by a third-party contractor, under Zetta Systems' supervision and procedures, following the **(NIST) Special Publication 800-88** prescripts.

5.5.2. After successful media sanitization, mediums are removed from Zetta Systems' hardware inventory.

6. Access and identity management

6.1. Authentication

Zetta Systems has strong password policy requirements and enforcement rules managed via centralized system providing AAA such as: Microsoft Active Directory, Microsoft AzureAD, AWS IAM and RADIUS:

6.1.1. Passwords or sensitive data must be stored in Zetta Systems' central password repository called **Password Manager** (PM).

6.1.2. Access to different resources, including client's related resources is controlled via ACL in the **Password Manager** and each person has different access levels, depending on his role.

6.1.3. **Password Manager** is storing historical data for any password changes, access level changes or access.

6.1.4. Each personal account of the employees has a password expiration policy requiring password change every **three (3) months**.

6.1.5. Each employee password meets the password complexity recommended by the **(NIST) Special Publication 800-118** guide.

6.1.6. Multi-Factor Authentication devices and algorithms are enforced on the system that have such support: web accounts, desktop accounts, VPNs

6.1.7. Passwords on the systems which are not compatible with AAA policy must be changed every three **(3) months**.

6.1.8. Master keys, API or tokens are rotated, renewed on regular basis

6.1.9. Sharing, exchanging common accounts, keys, tokens, or any other authentication digital signatures is prohibited

6.2. Authorization

Information access and permissions are controlled via different technologies and processes. Each of them must provide the right to use the information assets and determine what type of access is allowed Create, Read, Update and Delete (CRUD).

6.2.1. When AAA support is not available, local authorization rules and procedures are applied.
6.2.2. Access control depends on the system type, data classification or risk level of compromise.
6.2.3. Data owner(s) is responsible to grant/control and review the permissions every three (3) months.
6.2.4. Access to any distribution groups and internal systems is determined by the employee's lead, head of department or HR department.
6.2.5. Each employee is operating with a low-privileged account managed via the centralized AAA system, when AAA system is not supported, local system policies are applied.
6.2.6. DevOps engineers use low-privileged accounts managed via the centralized AAA system, when AAA system is not supported, local system policies are applied. High privileged accounts must be used only for configuration purposes and access to them is set to minimum.
6.2.7. Each employee is operating under low-privileged account for its day-to-day tasks
6.2.8. Zetta Systems has procedures controlling the authentication and authorization process when an employee is on boarding or leaving the company.
6.2.9. Each Zetta Systems system has session time-outs of user inactivity after which the session is locked or terminated.

6.3. Remote Access

6.3.1. Remote access to any internal Zetta Systems resources: workstation, infrastructure equipment and systems, password manager systems or any other management systems or any other data in motion is only permitted via secured, encrypted, and authenticated VPN session.
6.3.2. Tunnels are secured with **Public Key Infrastructure** (PKI).
6.3.3. Any other unauthorized methods providing remote access to the Zetta Systems infrastructure are prohibited.
6.3.4. VPN sessions to Zetta Systems network are established only with Zetta Systems' VPN approved clients. Any unapproved connection managers are subject to reject or terminate the VPN session immediately.
6.3.5. Zetta Systems' employees or third-party contractors are not allowed to copy any **company** or **client data** to which they have access.

7. Staff

7.1. Pre-Employment Background Checks

The Company will conduct employment reference checks, "investigative consumer reports" and background investigations on all candidates for employment prior to making a final offer of employment and may use a third party to conduct these background checks.

The type of information that will be collected by the Company in background checks may include, but is not limited to, some or all the following:

7.1.1. Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to suitability for employment
7.1.2. Education (including degrees awarded and GPA)
7.1.3. Employment history, abilities, reasons for termination of employment
7.1.4. Address history
7.1.5. Credit reports
7.1.6. Civil court filings

7.1.7. Motor vehicle and driving records
7.1.8. Professional or personal references

7.2. Employee Training and Awareness

Zetta Systems' employees are required to become acquaint with this policy and customer data protections as:

7.2.1. Each employee is binding on the policy and procedures when on boarding.
7.2.2. Each employee is acquainted with the latest policy and procedures changes
7.2.3. Each employee has internal access to each policy and procedure and can access the information on demand

7.3. Employees leaving the company

7.3.1. Zetta Systems has procedures controlling the authentication and authorization process when an employee is on boarding or leaving the company.
7.3.2. When an employee is leaving: ACL, PINs, security tokens, and any keys must be revoked.

7.4. Third party contractors

7.4.1. Zetta Systems is not exchanging any **customer-related data** with third party data vendors or contractors.

8. Security procedures

8.1. Framework practices

8.1.1. Zetta Systems Information Security Management System (ISMS) is aligned with the industry best practices and frameworks - **ITIL v3, rev. 2011** and **ISO 27001**.

8.2. Incident response and procedure

Following procedure must be observed in case of any security breach detection:

8.2.1. In case of security breach detection, all activity to the affected service must be isolated for further investigation and analyses by the **security team**.
8.2.2. Internal notifications and assessment reports are exchanged between the affected departments for risk categorization.
8.2.3. **The Chief Technology Officer** must contact all affected individuals and report the assessment report.
8.2.4. Acceptable notification time is **six (6)** hours after incident detection.
8.2.5. Execute business continuity plan

8.3. Auditing, Monitoring and Logs

Proper internal control is applied over all IT assets. Any security events related Zetta Systems' infrastructures are logged and monitored:

8.3.1. Each system uses a central repository for storing log records. When this is not possible, logs are kept locally.
8.3.2. Log retention period is **tree (3)** months.
8.3.3. Log deletion or modification is prohibited.
8.3.4. Monitoring is applied over any network devices, servers, workstations, and applications.
8.3.5. Authentication and authorized requests are tracked into the security audit log.
8.3.6. Remote VPN sessions are tracked into a centralized database.

8.4. Change Control

8.4.1. Zetta Systems logs and tracks all changes made to the software through its issue tracking system, which is used to ensure that changes to the products delivered to users of the hosting service are controlled and recorded.
8.4.2. Tracking provides a way to identify changes in the event of a security breach or data integrity issue.
8.4.3. Software revision list is kept
8.4.4. Any critical systems changes are controlled via **RFC**, advised after **CAB** or **ECAB** team meeting.

8.5. Vulnerability Protection

8.5.1. Industry standard firewalls with stateful inspection are filtering and applying different ACL policies over the inbound and outbound traffic.
8.5.2. Each workstation is protected by a local firewall and no exceptions are allowed.
8.5.3. Each workstation and critical system like file server have enterprise level **Antivirus System** with definition update on every six (6) hours.
8.5.4. A full system scan is performed on a weekly basis.
8.5.5. Zetta Systems is enforcing Antivirus policy and users are not allowed to stop or make any configuration changes to the Antivirus software.
8.5.6. Zetta Systems is using Microsoft 365 Advanced Threat Protection (ATP) - a cloud-based filtering service to protect against viruses and other malware, including zero-day attacks with the following enforced features - Policies, Safe attachments, Safe Links, Anti-phishing protection, Quarantine, Spoof Intelligence and Threat Investigation and Response.
8.5.7. Each employee operates under low-privileged account for his day-to-day tasks.
8.5.8. Operating systems are patched on a regular basis via Azure AD policies, Azure Security Center, and windows update center.
8.5.9. **Common Vulnerabilities and Exposures** (CVE) lists are monitored, and precaution steps are taken in case of major information-security vulnerabilities and exposures.

8.6. Vulnerability Analysis

Periodic penetration tests against Zetta Systems' infrastructure and online services (official website, bug-tracking and knowledge-based systems, password manager, etc.) are performed on every six (6) months:

8.6.1. **OWASP** based assessment tests against Zetta Systems' online services.
8.6.2. Network assessment security tests against Zetta Systems' infrastructure and online resources.
8.6.3. Testing results and reports for further analysis.

8.7. Bring Your Own Device (BYOD)

Zetta Systems' employees are authorized to use any mobile devices such as personal smartphones, tables, or laptops of their choosing at work for their convenience. Zetta Systems has full rights to revoke any access if the employees are not observing the policy specified:

8.7.1. Zetta Systems is not responsible for maintaining any security updates or patches released for the operating systems of the **BYOD**. Each employee must take care of the update maintenance and protection of its device.
8.7.2. **BYOD** are not allowed to join to the corporate network or domain.
8.7.3. **BYOD** are allowed to use only Zetta Systems' Guest network(s)
8.7.4. Zetta Systems is applying security policy for **remote wipe** and **PIN** screen lock requirements for mobile devices such as smartphones and tablets.
8.7.5. Zetta Systems has full rights to remotely wipe the **BYOD** in case the device is lost, or employee contract is terminated.
8.7.6. Any rooted BYOD such as smartphones and tablet are prohibited and are subject to terminate the access to Zetta Systems' resources.
8.7.7. Any **company** or **client data** transfer from and to the **BYOD** is prohibited.

9. Physical Control

Access control over Zetta Systems property, facilities and equipment is controlled via various techniques. Access list consistency is revised on yearly basis.

9.1. Office

Zetta Systems office meets the following requirements:

9.1.1. Security guard.
9.1.2. CCTV.
9.1.3. Access Control List
9.1.4. Security PINs or security token for each employee.
9.1.5. When employee is leaving: ACL, PINs, security tokens, and any keys must be revoked