Performance Objectives: Charts for Jira (https://performance-objectives.com/)

Powerful reporting app for Jira dashboards

SECURITY POLICY

10.Jan.2021

Last update: 07.Nov.2024.

Purpose and Scope

This policy document defines requirements for the appropriate and secure use of Sensitive Information at DevAcrobats Ltd.

Sensitive Information, for the purpose of this document and the policies herein, shall be defined as Client Data, Company Confidential Data, Personal Data and any combination thereof.

Client Data includes, but is not limited to, any data not otherwise generally available to the public that is made available to DevAcrobats by a Client, prospect, or authorized third-party for the purpose of delivering agreed-upon services, as well as any related information pertaining to the organizational or commercial operations of a Client or prospect that is not otherwise generally available to the public. All Client Data shall be handled as confidential regardless of content, and shall only be stored, accessed, disseminated or otherwise handled in accordance with legally executed agreements for services between DevAcrobats and its Clients, as well as all applicable laws.

Company Confidential Data includes, but is not limited to, any information pertaining to the organizational or commercial operations of DevAcrobats, its employees, contractors, agents, vendors, affiliates, business processes, proprietary technology and intellectual property, where such information was made available in connection with an individual's employment or association with DevAcrobats and is not otherwise generally available to the public.

Personal Data includes any type of personally identifiable information. **Employee**, for the purpose of this document and the policies herein, shall be defined as any individual DevAcrobats employee, contractor or agent using DevAcrobats workstations and/or personal mobile devices to handle Sensitive Information.

Comprehensive information about the type of personal and client data that is collected by or may be disclosed to DevAcrobats through the Performance Objectives: Charts & Reports for Jira Dashboards app's Service Management System, the company emails, and other sources can be found in our Cookie and Privacy Policy (https://performance-objectives.com/data-security-and-privacy-statement/).

The **Performance Objectives: Charts & Reports for Jira Dashboards app** does not collect and store client data. We collect usage statistics for the app (for both downloadable and Cloud versions). No Jira instances data and no personal data is collected through these usage statistics.

Application

This policy document applies to all DevAcrobats employees. Compliance with the policies in this document is mandatory. Employees may be held responsible for damages suffered by DevAcrobats or its Clients resulting from non-compliance.

Employee Workstations

Appropriate measures must be taken when using workstations (laptop and desktop computers) to ensure the security and confidentiality of Sensitive Information. DevAcrobats will implement the following safeguards for all workstations.

Security Measures

For Windows workstations, DevAcrobats utilizes management agents to automatically enforce these measures whenever possible.

- Asset Inventory
- Antivirus & Endpoint Protection
- Strong Passwords for Workstation access
- Automatic screen lock, Timeout of 15 min or less
- Critical and High Priority OS Updates
- Local Storage Device Encryption (AES-256)

Note: A “strong password” must be at least 10 characters in length and meet all of the following criteria:

- Contains at least one uppercase letter.
- Contains at least one lowercase letter.
- Contains at least one number.
- Contains at least one non-alphanumeric symbol.

Acceptable Use and Employee Responsibilities

Use of workstations to store, access or otherwise handle Sensitive Information shall be limited to workstations in compliance with this Policy. Employees who utilize workstations in an applicable fashion acknowledge responsibility to take all appropriate measures to protect Sensitive Information.

Employees will take appropriate protective measures, including the following:

- Restrict physical access to workstations to only authorized personnel.

- Avoid password sharing at all costs. If a password is being shared it must be a temporary password that is to be changed immediately after login.
- Use only DevAcrobats authorized workstations to carry out job responsibilities.
- Ensure 'Intune' management enrollment is in place if you have a Windows workstation.
- Secure workstations (screen lock or logout) prior to leaving an area to prevent unauthorized access.
- Report a lost or stolen workstation to employee's manager, IT Support .
- Do not work with sensitive information in crowded airplanes, trains, airports, cafes, hotel lobbies and other public spaces unless the workstation have privacy screen.

Personal Mobile Devices

There are no company mobile devices but appropriate measures must be taken when using personal mobile devices (smartphones, tablets, etc.) to ensure the security and confidentiality of any Sensitive Information. This policy applies to all personal mobile devices which are used to access to corporate email, and those used to access internal DevAcrobats resources. DevAcrobats employees must implement the following safeguards for all applicable personal mobile devices.

Security Measures

Each of the following must be user-managed**.**

- Password for Device Access
- Device-Level Encryption
- Automatic Screen Lock, Timeout Period of 15 minutes or less
- Critical and High-Priority OS Updates

Acceptable Use and Employee Responsibilities

Use of personal mobile devices to store, access, or otherwise handle Sensitive Information shall be limited to tasks which cannot be reasonably completed using a non-mobile device. Employees who utilize personal mobile devices in an applicable fashion acknowledge responsibility to take all appropriate measures to protect sensitive information.

Employees will take appropriate protective measures, including the following:

- Enable password/passcode protection for device access.
- Enable device-level encryption.
- Enable auto lock-out mechanism with a timeout of 15 minutes or less, where not automatically enforced on the device.
- Enable out-of-band location tracking for the device, with the ability to lock or disable the device remotely.
- Apply critical and high-priority operating system and application updates in a timely manner.
- Ensure the device's native security and platform controls are not subverted via "jail-breaking."
- Report a lost or stolen device to employee's manager and IT immediately.
- Do not work with sensitive information in crowded airplanes, trains, airports, cafes, hotel lobbies and other public spaces unless the workstation has a privacy screen.

Network Access Considerations

There are no trusted DevAcrobats wired or wireless networks. Employees must exercise the following practices when connecting workstations or personal mobile devices to a network for the purpose of carrying out assigned responsibilities. Employees should exercise appropriate due diligence when connecting to any network. Make sure they are trusted networks and not insecure coffee shop connections, it is acceptable to hotspot from your phone if necessary.

Handling of Sensitive Information

DevAcrobats employees should not use workstations, personal mobile devices, and/or cloud storage to store, access, or otherwise handle Client Data and/or Company Confidential Data shall consider the sensitivity of the information and minimize the possibility of unauthorized access or use. Employees will take appropriate protective measures, including the following:

Acceptable Use

Employees who become aware of unnecessary or incidental access to Client Data or Company Confidential Data for themselves or others shall promptly report it to their manager and the responsible party for remediation.

Transfers

Any data should be transferred using encrypted means of transit (HTTPS, SFTP, etc.). Transfers via email should only be used when the Client has no viable alternative.

Storage

Employees storing Client Data locally on workstations or personal mobile devices shall only do so on an as-needed basis for the purpose of carrying out tasks authorized by the Client.

Client Data shall be deleted from workstations and personal mobile devices at the conclusion of the engagement.

Client Data and Company Confidential Data must be stored on an encrypted storage device.

Client Data and Company Confidential Data shall not be stored on removable media.

Employees storing Client Data and/or Company Confidential Data on cloud-based storage shall only use cloud-based storage services approved for corporate-wide use. At current limited to Google, GitHub, Jira.

Client Data shall be deleted from cloud-based storage in accordance with all applicable Agreements for Services.

Compliance and Support

Compliance with the policies set forth in this document is verified through various methods, including periodic internal audits and automated reports. Any exception must be approved in writing by responsible parties listed below.

This policy document applies to all DevAcrobats Employees. Compliance with the policies in this document is mandatory. Employees may be held responsible for damages suffered by DevAcrobats or its Clients resulting from non-compliance.

Security Self Assessment

The policy complies with the CAIQ-Lite security self assessment (https://performance-objectives.com/security-self-assessment-caiq-lite/) done by DevAcrobats.

Policy Management

Questions about the purpose and content of this policy document should be directed to the following parties:

INFORMATION SECURITY:

Operations Manager: operations@devacrobats.com

Technical Support

Questions about how to implement specific security measures should be directed to IT support: support@devacrobats.com

PRIVACY (HTTPS://PERFORMANCE-OBJECTIVES.COM/DATA-SECURITY-AND-PRIVACY-STATEMENT/)

SUPPORT (HTTPS://DEVACROBATS.ATLASSIAN.NET/SERVICEDESK/CUSTOMER/PORTAL/1)

MARKETPLACE (HTTPS://MARKETPLACE.ATLASSIAN.COM/APPS/1218655/PERFORMANCE-OBJECTIVES-CHARTS-REPORTS?TAB=OVERVIEW&HOSTING=CLOUD)

SLA (HTTPS://PERFORMANCE-OBJECTIVES.COM/SERVICE-LEVEL-AGREEMENT-SLA/)

EULA (HTTPS://PERFORMANCE-OBJECTIVES.COM/END-USER-LICENSE-AGREEMENT/)

SECURITY (HTTPS://PERFORMANCE-OBJECTIVES.COM/SECURITY-POLICY/) STATUS (HTTPS://DEVACROBATS.STATUSPAGE.IO/)