datarails

Information Security Policy

January 2023

Introduction

Datarails is A Financial Planning and Analysis Solution for Excel users.

Datarails automates data consolidation, reporting and planning, while enabling finance teams to continue using their own Excel spreadsheets and financial models.

Automating these time-consuming manual processes paves the way for finance teams to spend more time analyzing data and less time collecting it. It also empowers them to answer essential strategic questions like what their organization can do to increase revenue and reduce expenses.

Continue working in your Excel environment exactly as you work today, with full functionality and flexibility – but a lot less time spent on manual data collection or copy and paste. Customize your reports and control how your data is structured, no matter how it's stored in the original source. Keep your spreadsheet formats, formulas, and financial models or change them; you have full control.

1. Purpose and Scope

This security policy describes Datarails' leadership view of information security and its implementation in the vision, strategy and day-to-day activities of the company.

The security policy provides high-level guidelines for practicing information security in Datarails. Further details regarding the implementation of various information security aspects can be found in Datarails' security procedures.

This security policy relates to Datarails' Production facilities and to Datarails' corporate offices worldwide. The policy refers to all systems, networks and data resources operated and managed by Datarails.

Information Security is part of Datarails' core and strategic goals. The following concepts are part of Datarails' security outlook:

- Providing trusted service to Datarails' customers by protecting their data assets that are hosted and processed as part of Datarails' services.
- Protecting privacy throughout the operations.
- Coplay with and adhere to various industry standards and applicable laws

Security at Datarails is part of the overall ownership that each employee is required to demonstrate at all times.

Datarails' Leadership is committed to maintaining an adequate level of information security and intends to invest the required resources to enforce its security policy in all aspects of the company's activities.

All Datarails employees, consultants, contractors and affiliates are subject to the policies noted herein. Continued lack of adherence to the policies

may result in appropriate disciplinary action, up to and including termination of employment or affiliation.

2. Ownership

Developing and maintaining this policy is the CSO's ownership.

Datarails leaders are responsible for enforcing this policy within their groups and the day to day operations.

3. Vertical Security Ownership

Security at Datarails is part of everyone's ownership and responsibly. The following table outlines Datarails' leadership expectations from major groups within Datarails:

R&D	Follow secure coding and testing practices
Product Management	Develop future plans and features related to security, research business cases related to Datarails platform security.
Operations	Maintain secure infrastructure and systems
Sales & Customer Success	Secure connection and communication with prospects and customers, protection of their information and escalation of issues and potential incidents reported by customers
HR / People Group	Protect individuals and employees privacy and employment related data.

4. Organizational Structure

Datarails' CEO delegates the overall security responsibility and authority at Datarails to the Chief Security officer (CSO).

4.1 Chief Security Officer

The Chief Security Officer (CSO) holds the highest responsibility and authority regarding Information Security in Datarails. The CSO will lead the Datarails Security team.

4.2 Formal Security team duties:

- Defining Datarails' information security strategy.
- Establish and maintain Datarails' security policy.
- Setting the security standards for Datarails networks and systems.
- Assisting business owners with developing security enhancements to the service.
- Helping the Development groups maintain secure coding best practices.
- Defining required security mechanisms, and managing their implementation.
- Assisting with processes related to security incident response.
- Managing the security due diligence processes with customers (RFP's, audits)
- Maintaining ongoing risk assessments for Datarails.
- Maintaining a security awareness program.
- Maintaining ongoing operational cycles such as BCP, compliance, risk assessment.
- Supporting data owners with protecting their data assets.

4.3 Security team

The security team will help the CSO to implement the security policies and the roadmap that was approved by the Datarails management.

The security team members need to know or have:

- At least 7 years of experience in the security field
- Need to have strong knowledge in the fields of:

- Access Control
- Application Development Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations and Compliance
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

4.4 Datarails' Data Assets

The following data types are Datarails' data assets:

- Customers' data: any data related to Datarails' customers. The data can be obtained as a by-product of interaction and engagement (support, PS, sales) or data that is processed and stored by Datarails' service and application.
- Datarails' application source code and raw data.
- Product related data: business plans, competition, new features.
- Individual Private Data (People): social security numbers, ID, salary, health, performance, and recruitment.
- Financial data: any nonpublic data that might have impact on Datarails' reports, stocks and other financial operations.
- Infrastructure and systems: servers and applications that support, process or maintain the Datarails services.

4.5 Responsibility for data assets

- #### Data asset owners

  Each data asset will be owned by an appropriate data owner that will be approved by Datarails leadership. The data owner must be a Datarails employee.

- #### Information asset owner's responsibilities

  Data asset owners are responsible to maintain the appropriate security controls of their data assets, consult with the Security team on implementation of such controls, and reporting any security incidents related to their assets.

5. Information Classification and Sensitivity

Datarails believes that policies should be simple, therefore all Datarails information is categorized into two main classifications: Datarails Public and Datarails Confidential. If an employee is uncertain of the classification of a particular piece of information, he or she should contact their leader.

5.1 Datarails Public Information

Datarails Public information is information that has been declared public knowledge by the information asset owner or by the CSO. This information can be freely given (modified?) to anyone without any possible damage to Datarails.

5.2 Datarails Confidential Information

Datarails Confidential information contains all other internal information or data. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very

closely, such as customers' data, personally identifiable information (PII), trade secrets, development programs, potential acquisition targets, and other information integral to the success of our Company.

A subset of Datarails Confidential information is "**Datarails Third Party Confidential**" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Datarails by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier or vendor into Datarails' network to support our operations.

6. Acceptable Use

The usage of Datarails' network and all data assets or systems is subject to Datarails' acceptable use policy. Any use of external systems or devices to process or transmit Datarails data is subject to this information security policy and the acceptable use policy.

All new and existing users should be aware of the acceptable use policy and accept it prior to using Datarails' network, data assets and systems. The summary of acceptable use policy will be presented to new employees as part of the Datarails welcome experience for new hires.

Customer data will be reside only in the Datarails Production network. The access to the data is granted on the need to work basis and least privileges concept. Datarails prohibit transferring customer data outside the production network, unless the customer approved this as part of support process.

7. Access control

7.1 Role Based Access Control

Access to Datarails data assets is restricted, and will be granted to Datarails employees and contractors in order to fulfill their duties on a need-to-work basis (least privileged approach). Permissions will be granted based on roles (RBAC) with minimal access.

By default, contractors and 3rd parties are not allowed to directly access customers' data.

7.2 Accountability

Each Datarails user is personally accountable for his/her actions in regard to Datarails data assets. Each activity performed in Datarails' data assets is assigned to the user who has performed it.

Any Datarails user that will not comply with Datarails' security policy and Datarails' Acceptable Use Policy shall be personally responsible for this non-compliance.

7.3 User Account Management

Usage of Datarails' systems and data assets will be performed through personal user accounts only. Users shall not allow other users to use their user accounts, or use user accounts of other Datarails users.

Non personal user accounts (Generic accounts) are not acceptable since the usage of such accounts prevent accountability for actions. Exception will be considered by Security team.

Further information regarding user account management can be found in the "User Management" procedure.

7.4 User Authentication

Authentication is the main security control for maintaining an appropriate level of security for data assets. The authentication methods in use are outlined in the Datarails' User Management procedures, and are set based on data sensitivity and risk assessment.

Users are required to login to Datarails' systems in order to access their accounts. Authentication data and devices (e.g. passwords, authentication tokens) provided by Datarails are meant for the individual use of the user receiving them.

8. Password Policy

Employees at Datarails must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of IT's strategy to make sure only authorized people can access those resources and data.
All employees who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorized people.
The purpose of this policy is to make sure all Datarails resources and data receive adequate password protection. The policy covers all employees who are responsible for one or more account or have access to any resource that requires a password.

8.1 Password creation

- All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.

- In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective.
- A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase “This may be one way to remember” can become “TmB0WTr!”.
- Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.
- All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.
- If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they’re initially set up — must be changed as quickly as possible.

8.2 Protecting passwords

- Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

- Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognize these attacks.
- Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.
- Employees may not use password managers or other tools to help store and remember passwords without IT's permission.

9. Encryption

9.1 Encryption - Policy

In a data-centric approach and operations, encryption has a key-role for data protection. Encryption will be utilized by Datarails as a part of the overall security mechanisms to protect internal and customer's data.

Confidential information will be encrypted while transmitted over external networks. All network communication channels between Datarails' offices and the production network will be established through an encrypted tunnel (site to site VPN)

Encryption will be based on well-known industry standard algorithms that support appropriate key-management processes. Confidential data stored within Datarails' DB servers will be encrypted with AES encryption as a minimum standard for customers who require encryption for data at rest.

Authentication related information such (e.g. passwords) must not be stored in clear text. The use of a one-way hash function to irreversibly encrypt such data is required.

10. Security Incident Reporting

Any event or incident that might impact Datarails' data or systems security should be reported by every employee to data owners and security team via security@Datarails.com in order to promptly mitigate the risk.

11. Incident Response

Security incidents detected by Datarails employees, customers or business partners shall be reported to the Datarails Security team. The incident response will be based on Datarails' "Security Incident Response" procedures.

12. Ongoing Risk Assessment

Ongoing risk assessment processes are part of Datarails' security program. The purpose of the risk assessment is to (1) identify potential security risks within Datarails' environment (2) assess the potential business and security impact and (3) define the gap remediation ownership and plan.

Leaders, System owners and Data owners are responsible for the development and implementation of a remediation plan within Datarails' various business units, in accordance with the-CSO instructions and risk assessment results.

13. Independent Penetration Testing

Datarails conducts periodic security testing of its service, systems and data assets. The testing is performed by an independent 3rd party security

experts according to the scope and schedule described in the "Secure Development Lifecycle" Procedure.

14. Communication Security

14.1 Communication over the Internal Network

- **Perimeter protection:**

  Datarails' network and data assets are surrounded by the Datarails perimeter. The perimeter is implemented using various communication and security technologies and mechanisms (e.g. Firewalls, routers). The perimeter prevents unauthorized access to Datarails information assets by external entities, and prevents leakage of Datarails information assets to the outside world.

- **Network Segregation and Segmentation**

  Datarails' network is divided into three segregated network environments:
  The development network, the testing and staging network, and the production network. Each of these environments is segregated from the other environments, and has its own privilege allocation and access control. Transfer of data between these environments is subject to Datarails' Environment Separation procedures and Change Management procedure.

- **Limited access by external entities**

  Access to Datarails' network and information assets by non-Datarails employees is restricted. Only specific access that is essential to the successful operation of Datarails' service is allowed. All access by external entities needs to be reviewed by the Security team and is subject for its approval.

- **Concurrent Network Connections**

  Establishing concurrent wireless (WiFi) and wired (e.g. Ethernet) connections is prohibited and should be technically restricted where applicable.

14.2 Communication over external channels

Communication based on public or external channels (e.g. the Internet) transferring Datarails confidential information is encrypted using an industry known standard encryption. The use of encryption is subject to the relevant governing laws and regulations in each country Datarails operates in.

- **Cloud and SaaS**

  In addition to the obvious benefits of cloud computing, hosting internal data out of Datarails' network involves various risks, and must be done with caution. The usage of cloud based and SaaS based systems is subject to the guidelines outlined in Datarails' Security Guidelines for Cloud Computing.

- **Remote Access**

  Remote access to Datarails systems and data assets that are hosted at Datarails premises requires an encrypted connection over VPN. The access type and permissions are determined based on least privileges, role based and need to work basis.

- **DMZ Policy**

  Datarails networks connected to external networks are protected with Network Firewalls.

  No incoming or outgoing communication is allowed, unless screened by a firewall according to rules approved by the Security team and Director

of Production Operations. Exceptions based on risk assessment will require approval by the CSO.

Direct access from Internet to LAN is prohibited and will be established though DMZ network. The DMZ will include web servers that will use as proxy to application servers.

Incoming traffic entering Datarails' application servers will be monitored, validated and screened by an application level filtering mechanism before transition to any production application server in order to prevent application level attacks.

Network management will be established through a separated Out-Of-Band management segment. Servers within the DMZ will comply with Datarails' Server Hardening Standard. External penetration tests will be executed by an external 3rd party at least on annual basis.

Changes affecting the level of security should be evaluated by the CSO/ Security team according to the Datarails Change Management policy.

15. Human Resources Security

- All prospective employees go through pre-employment reference and/or background checks, in accordance and compliance with the local HR policies and applicable national laws.
- All employees sign a non-disclosure agreement and accept the employee manual, the security policy and the acceptable use procedure when their work commences.
- Any change in an employee's position in Datarails or change in his/her access privileges is reported to the CSO and documented by HR.
- Termination of an employee's employment is reported to Security and system owners, who revoke the user's access and accounts on a timely manner.

16. Security in the Development Lifecycle (SDLC)

16.1 Secure development practices

Information Security aspects are considered in major phases of the development lifecycle, from the initial design and up to the final testing. Software development in Datarails is performed according to the "Security in the development lifecycle" procedure.

16.2 Security testing

Detecting security issues are one of the goals for software testing in Datarails. Test plans and test cases for new versions include security testing as an integral part of the test process. Security testing is performed as part of the testing process throughout the development lifecycle, according to the “Security in the development lifecycle" procedure.

17. Change Management

Datarails' application and networking environment is dynamic, to support the changing needs of its customers and the ever-growing requirement for capacity and performance.

Changes to Datarails' application or networking environment that may have impact on the platform security - require security clearance from the CSO. Other changes must be executed according to the Datarails Change Management procedure.

18. Physical Security

The physical security of Datarails' facilities (offices, datacenters) is an essential part of Datarails’ security standards. Employees, contractors, and visitors are subject to the requirements set forth in Datarails’ Physical Security procedures.

19. Legal and Regulatory Compliance

Datarails operates in various countries worldwide and is subject to multiple sets of laws and regulations regarding information security.

Datarails' Legal Department remains apprised of and evaluate new legal and regulatory requirements applicable to Datarails' business, and updates, recommends or implements compliance policies and procedures as needed in coordination with other groups throughout the Company.

In case of conflict between this policy and local or federal laws and regulations, Datarails will adhere to strictest requirement (either in the policy or laws), always complying with or over-performing the legal requirements.

20. Awareness and training

Security awareness is a key factor in maintaining an effective security program. Upon commencing work at Datarails, employees receive security briefing and relevant datasheets. Security awareness materials and training are communicated to employees on regular basis. Security content is communicated to new employees as part of the welcoming experience. On annual basis, all Datarails employees are required to complete security training.

21. Audit

21.1 System and operations audit

The use and activity of Datarails confidential information assets shall be logged and audited for security incidents and non-compliance with Datarails' security policy. Datarails' infrastructure and operations undergo an annual security audit by independent 3rd party auditors.

21.2Policy and Procedure audit

Datarails' Security team performs an annual review of the security policy, security procedures and the company's compliance with these documents. This review outlines potential problems, proposed changes and improvements.

22.Document Ownership

The CSO is the owner of this document and is responsible for ensuring that this policy is reviewed and approved. A current version of this document is available to all Datarails employees at the Datarails Online Community.