Eventopolis – Data Security Policy

# Table of Contents:

|  |  |  |
| --- | --- | --- |
| Sr. No. | Title | Page No. |
| 1 | Statement of Purpose |  |
| 2 | Applicability |  |
| 3 | Objectives and CIA Triad |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 1. Statement of Purpose

This security policy establishes the framework for safeguarding the decentralized blockchain and smart contracts-controlled data sharing platform within Eventopolis, implemented using the SentinelShare web application. Its primary goal is to ensure information integrity, data privacy, and regulatory compliance through effective security measures.

# 2. Applicability

This policy applies to all personnel within the organization hierarchy, including any individuals/groups/organizations serving under a contract with Eventopolis:

1. **The CEO**
2. **Other C-level Executives** - CTO, CFO, CISO, CHRO
3. **Horizontal Heads** (Hospitality, Public Relations, Logistics, Technology, and Security)
4. **Project Managers** ( specific for each new event)
5. **Vertical Heads** (specific for each of the departments for every event being planned)
6. **Executives** (the team under the vertical heads, responsible for carrying out the operations)
7. **Third-party vendors** (being contracted by the company)
8. **Clients**

Access to the general public is regulated solely through the deficit of any data security and privacy controls, as will be illustrated in the Data Classification section of this document.

# 3. Objectives and CIA Triad

The security policy aims to achieve the following objectives, encompassing the Confidentiality, Integrity, and Availability (CIA) triad:

- Establish and communicate the importance of information security within Eventopolis.

- Securely manage data sharing through blockchain technology and smart contracts.

- Implement multi-user access with role-based authentication to ensure data confidentiality and efficient access management.

- Enable fine-grained file identification and classification through attribute-based access control (ABAC).

- Implement metadata management for compliance, data ownership, and access control.

- Ensure secure data transmission through encryption and end-point security measures, including measures for third-party risk management for vendors, contractors, clients, and such.

- Create a real-time notification system for policy violations and breaches to facilitate business continuity and recovery.

- Align data classification with roles and implement automated classification mechanisms.

# 4. Data Classification

Data is categorized into levels of sensitivity, including Top-Secret, Secret, Confidential, Restricted, Internal, and Unclassified.

Top-Secret Data:

Top-secret data refers to the highest level of sensitive information within Eventopolis. This category typically includes data that, if disclosed or compromised, could have catastrophic consequences for Eventopolis or its stakeholders. Access to top-secret data is highly restricted and limited to a select group of individuals with the highest level of authority and clearance within Eventopolis. Unauthorized access or disclosure of top-secret data can result in severe legal consequences.

Secret Data:

Secret data is classified as highly sensitive and valuable information, although not as critical as top-secret data, within Eventopolis. It includes information that, if exposed, could still cause significant harm to Eventopolis or its interests. Access to secret data is granted to individuals who have a legitimate need to know and have been authorized to access this level of information within Eventopolis. Strict security measures are in place to protect secret data from unauthorized access.

Confidential Data:

Confidential data represents sensitive information that, while not as critical as secret or top-secret data, still holds considerable value and should be protected from unauthorized disclosure within Eventopolis. This category often includes proprietary business data, financial information, and customer data. Access to confidential data is typically limited to employees or stakeholders within Eventopolis who require it for their job responsibilities.

Internal Data:

Internal data refers to information that is essential for Eventopolis' day-to-day operations and decision-making but is not as sensitive as confidential, secret, or top-secret data. It may include internal communications, reports, and non-sensitive Eventopolis documents. Access to internal data is generally granted to Eventopolis employees and individuals who need it to perform their duties under a specific event project.

Restricted Data:

Restricted data includes information that is sensitive and should not be made publicly available but is not as critical as confidential, secret, or top-secret data within Eventopolis. This category often includes data shared with third-party vendors, partners, or specific stakeholders on a need-to-know basis. Access to restricted data within Eventopolis is tightly controlled, and individuals are given access based on their specific roles and responsibilities.

Unclassified Data:

Unclassified data is information that poses little to no risk if disclosed to the general public or individuals without a specific need to know within Eventopolis. This category includes publicly available information, such as marketing materials, public-facing Eventopolis websites, and non-sensitive public records. Unclassified data is typically accessible to anyone within Eventopolis and does not require special authorization or clearance to access.

Each level corresponds to specific roles within the organization, as detailed in the next section.

# 5. Authority and Access Control Policy

Access to data and resources is structured as follows:

**- All C-level Executives:** Access to top-secret level data and below.

**- Horizontal Heads:** Access to secret level data and below.

**- Project Managers and Vertical Heads**: Access to confidential level data and below.

**- Executives**: Access to internal level data and below.

**- Third-party vendors and clients**: Access to restricted data and below.

**- General public**: Access to unclassified data.

{diagram}

# 6. Data Use and Handling

All data usage and handling actions will be logged on the SentinelShare decentralized database located on a private Ethereum test-net.

The specific functions, with instances, and associated metadata, which will be encrypted per SentinelShare’s standards are enlisted below:

Data creation: Creation of data will all be logged with:

1. The unique identifier string of the entity that created it
2. The timestamp of creation
3. Type of data created (Files/Memos/Invoices/Reports/Plans of Actions/Forms)
4. Location of the data on the remote database
5. Classification level (Top-Secret/Secret/Confidential/Restricted/Internal/Unclassified)
6. Classification type (Manual/Automated)

Data handling adheres to data protection regulations, backup requirements, and network security standards. Encryption protocols are used for secure data communication. Policies cover data creation, classification, updates, deletions, and provisioning actions logged on the blockchain.

# 7. Responsibilities and Oversight

The MD and CXOs bear the responsibility of endorsing and overseeing policy implementation. Managers at various levels are accountable for enforcing security measures within their purview. Security incidents are reported to designated authorities for timely resolution.

* Acceptable Use Policy (AUP): This policy [governs how employees can use a website, network, or internet service](https://www.powerdms.com/policy-learning-center/updating-your-acceptable-use-policy). It might outline, for example, what types of files users can upload or download, or might prohibit harassing others or leaking company information. You might want to check out the detailed example from the [SANS Institute](https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy) of what an AUP looks like.
* Access Control Policy (ACP): This policy outlines who has access to what information within your company and how this is monitored and controlled. To get a feel for what an ACP looks like, you might want to check out this example from the [International Association of Privacy Professionals](https://iapp.org/media/pdf/resource_center/AWPHD-ISaccess.pdf).
* Passwords: This policy highlights what rules and processes you put around password security. For example, what are your requirements for safe passwords and how often should employees update them?
* Antivirus Software: This policy emphasizes whether or not antivirus software is required on each employee’s computer and explains why or why not.
* Remote Access: This lays some ground rules on whether workers can access sensitive data outside the office firewall or if they need a virtual private network (VPN) to securely access corporate resources. It also addresses access issues pertaining to mobile devices.
* BYOD (Bring Your Own Device): This policy delineates how and [when employees can use their own technology](https://www.powerdms.com/policy-learning-center/byod-policy-best-practices) to conduct company business and access company information.
* Auditing and Policy Review: This underscores how – and how often – you’ll monitor and review your IT security policy. Because threats are constantly changing, this policy needs to be “a living document” that is regularly reviewed to ensure it stays up-to-date.
* Enforcement: This explains how you plan to hold people accountable for following your computer security policies and procedures. It also clarifies what actions you’ll take if they don’t comply.

Because you can’t take a one-size-fits-all approach to develop an information security policy, you might need to include some additional elements depending on your individual circumstances. For instance, you might need to include policy components such as:

* Security Profiles
* Physical Security
* Monitoring and Intrusion Detection
* Disaster Recovery