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, CISO
3. **Horizontal Heads** (Hospitality, Public Relations)
4. **Project Managers** (specific for each new event)
5. **Vertical Heads** (specific for each of the departments for every event being planned)
6. **Third-party vendors** (being contracted by the company)
7. **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.

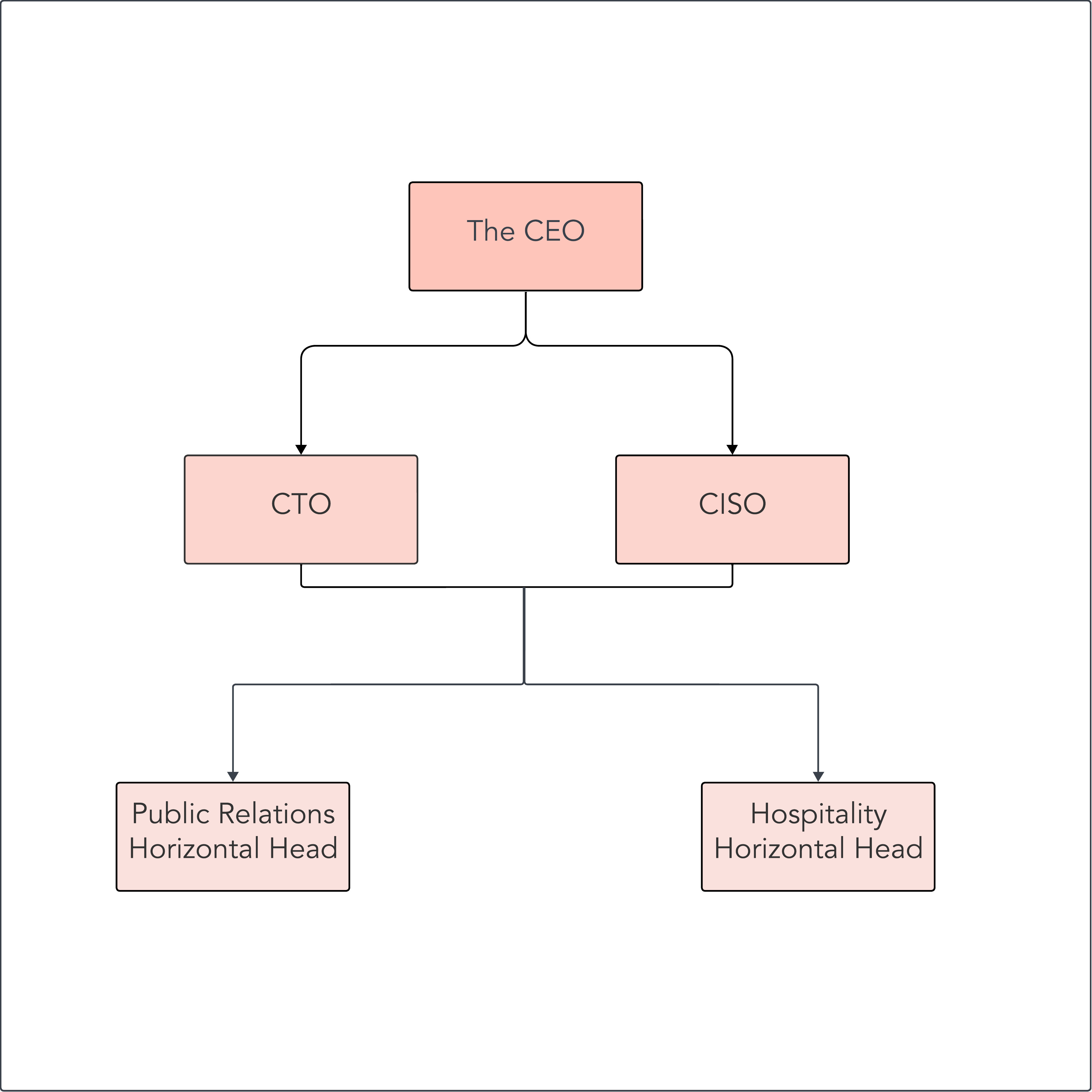


Diagram 1: General Company Hierarchy

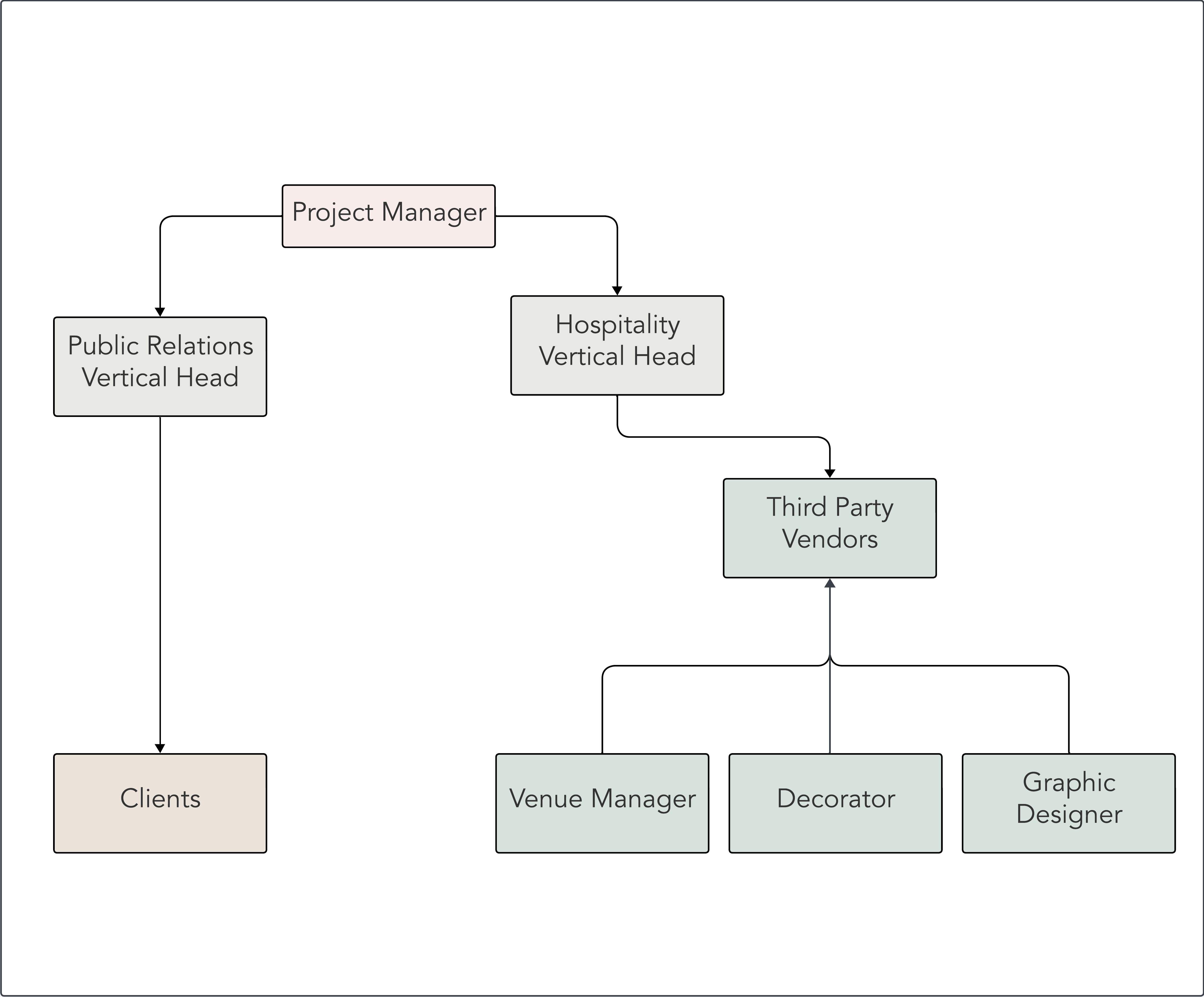


Diagram 2: Hierarchy established for the duration of a project //***update this***

Refer to Diagram 3 to establish the distinction between the Levels of the Hierarchy and the Levels for Data Classification.

# 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 in the company is classified into the following levels:

Secret Data:

Secret data is classified as highly sensitive and valuable information, very critical within Eventopolis. It includes information that, if exposed, could 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 secret level data and below.

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

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

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

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

{circle 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:

{Use Cases created to limit the Scope of Work for this project}

**Use Case 1:**

Login to Portal

Step 1 – Login ID, Password

Step 2 – OTP

Step 3 – Authenticate and Provide Access

**Use Case 2:**

New Project from Client

Step 1 – Use Case 1

Step 2 – ‘Request New Event’ Button

Step 3 – Client enters the following information:

Event Date,

Event Time,

Event Type (formal/ casual/ party/ wedding),

Theme Type (dark/ warm/ light/ pastels/ monochrome),

Venue Type (small/ medium/ big/ large),

Guest List (yes -> [Guest Name/ Guest Phone/ Guest Email]/ no)

Step 4 – Submit

**Use Case 3:**

Vertical Head (Hospitality) Assigning Work to Vendors (Venue Manager/ Decorator)

Step 1 – Vertical Head (Hospitality): Use Case 1

Step 2 – Vertical Head (Hospitality) sees the following on their dashboard:

Event Date,

Event Time,

Event Type (formal/ casual/ party/ wedding),

Theme Type (dark/ warm/ light/ pastels/ monochrome),

Venue Type (small/ medium/ big/ large)

Step 3 – ‘Assign to Venue Manager’/’Assign to ‘Decorator’ respectively

Step 4 – Submit

Step 5 – Vendor: Use Case 1

Step 6 – Vendor sees the following on their dashboard:

If Vendor.Type == ‘Decorator’:

Event Date,

Event Time,

Event Type (formal/ casual/ party/ wedding),

Theme Type (dark/ warm/ light/ pastels/ monochrome),

Venue Type (small/ medium/ big/ large)

Else If Vendor.Type == ‘Venue Manager’:

Event Date,

Event Time,

Venue Type (small/ medium/ big/ large)

Step 7 – Vendor adds the following information on their dashboard:

If Vendor.Type == ‘Decorator’:

‘Approved’/ ‘Rejected’

Else If Vendor.Type == ‘Venue Manager’:

‘Approved’ -> ‘Add Venue Address’/ ‘Rejected’

Step 8 – Submit

Step 9 – Vertical Head (Hospitality): Use Case 1

Step 10 – (Step 2) + Vendor Response ‘Event Venue Address’

Step 11 – ‘Approve’

Step 12 – Submit

Step 13 – Client: Use Case 1

Step 14 – Client sees contents from (Step 2) and Event Venue Address

Step 15 – ‘Approve’

**Use Case 4:**

Vertical Head (Public Relations) Assigning Work to Vendor (Graphic Designer)

Step 1 – Vertical Head (Public Relations): Use Case 1

Step 2 – Vertical Head (Public Relations) sees the following on their dashboard:

Event Date,

Event Time,

Event Type (formal/ casual/ party/ wedding),

Theme Type (dark/ warm/ light/ pastels/ monochrome),

Venue Type (small/ medium/ big/ large)

Event Venue Address

Step 3 – ‘Assign to Graphic Designer’

Step 4 – Submit

Step 5 – Vendor: Use Case 1

Step 6 – Vendor sees the following on their dashboard:

Event Date,

Event Time,

Event Type (formal/ casual/ party/ wedding),

Theme Type (dark/ warm/ light/ pastels/ monochrome),

Event Venue Address

Step 7 – Vendor adds the design files in .png/.jpg/.jpeg/.ai/.ps/.zip format on their dashboard

Step 8 – Submit

Step 9 – Vertical Head (Public Relations): Use Case 1

Step 10 – (Step 2) + Vendor Response files of ‘Invitation Design’

Step 11 – ‘Approve’

Step 12 – Submit

Step 13 – Client: Use Case 1

Step 14 – Client sees contents from (Step 2) and ‘Invitation Design’

Step 15 – ‘Approve’

**Use Case 5:**

Graphic Designer Attempting to Escalate Privilege by Requesting Additional Data

Use Case 4’s Steps 1 to 6

Step 7 – Vendor fills a ‘Data Requisition’ form on another tab on the dashboard, and enters the following:

Data Required = “Guest Names”

Reason = “To put on the invitations, so that they seem more customised and appropriate for such a personal event.”

Step 8 – Submit Data Requisition Form

Step 9 – Vertical Head (Hospitality) sees the Data Requisition form on their dashboard

Step 10 – Vertical Head (Hospitality) clicks on ‘Approve’/’Deny’

Step 11 – Submit

Step 12 – Project Manager: Use Case 1

Step 12 – Project Manager sees the Data Requisition form submitted by the vendor on their dashboard along with the Vertical Head (Hospitality)’s approval or denial of the request.

Step 13 – Project Manager clicks ‘Approve’/’Deny’

Step 14 – Vendor: Use Case 1

Step 15 – Vendor sees the approval or denial of the request basis this algorithm:

If Step 10 == ‘Approve’

If Step 13 == ‘Deny’:

‘Denied’

Else

‘Approved’ and Guest List table visible.

Else if Step 10 == ‘Deny’

If Step 13 == ‘Approve’:

‘Approved’ and Guest List table visible.

Else

‘Denied’

Step 16 – Use Case 4 Step 7 onwards.

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.