**Biotech Company Situational Analysis**

**Project 2**

Harrisburg University of Science and Technology

ISEM 547 IT Management

French Williams

July 19th

Rajan Pawar

Suraj Pratap Samirlal Poddar

Vikas Reddy Sarasam

Vishnu Vardhan Pisati

Dan Sun

Table of Contents

[Biotech Company Situational Analysis-Project 02 3](#_Toc77612017)

[IT Governance matrix 3](#_Toc77612018)

[Part B-Charter for the enterprise security committee 6](#_Toc77612019)

[Enterprise security committee 6](#_Toc77612020)

[Purpose 6](#_Toc77612021)

[Jurisdiction 6](#_Toc77612022)

[Objectives 6](#_Toc77612023)

[Responsibilities 6](#_Toc77612024)

[Decision authority 7](#_Toc77612025)

[Membership 7](#_Toc77612026)

[Deliverables 7](#_Toc77612027)

[Structure 7](#_Toc77612028)

[Relationships 7](#_Toc77612029)

[Executive signatures and dates 7](#_Toc77612030)

[Part C:Information Security Policy- IT data classifications 8](#_Toc77612031)

[Policy Statement 8](#_Toc77612032)

[Purpose 8](#_Toc77612033)

[Scope/Jurisdiction 9](#_Toc77612034)

[Objectives 9](#_Toc77612035)

[Definitions 9](#_Toc77612036)

[Policy Requirements & Controls 9](#_Toc77612037)

[References 10](#_Toc77612038)

# **Biotech Company Situational Analysis-Project 02**

## **IT Governance matrix**

An IT governance matrix is a paradigm to ensure that all functions are made clear concerning a company’s technological setup. It is important to ensure that it is embraced to safeguard the assets and functions of employees and generally improve the company’s output in terms of technological services. Below is an example of the matrix to be used in a company that lacks a governance structure that helps in ensuring that there are convenient operations (Nagar, 2018).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Governing Body** | **Purpose** | **Scope/Jurisdiction** | **Responsibilities** | **Decisions** | **Deliverables** | **Members** |
| Business & IT Executive Board | To oversee the IT department and make decisions on better directions. | Managerial area of the organization in the IT lane. | Make executive decisions for the IT sector. Oversees departmental deals. Ensure there is governance within the organization. | Financial implementations are necessary to the department. Hire and firing decisions in the department. Assign roles to leaders of IT entities. | Employee cohesion paradigms.  Financial approvals for departmental updates. | CEO, Company president, IT manager, and chief IT engineer. |
| Data/Information Committee | To monitor data incoming and exiting the company. | IT sector of the organization. | To monitor incoming data.  Filter data exiting the company. Communicate changes in the company. Manage data classifications. | They decide on how information should be classified.  Evaluate data importance to the organization. | Data maintenance updates. Information evaluation motifs for the organization’s data motifs. | Data analysts.  IT managers  Business system analyst. |
| Enterprise Application Committee | To streamline business applications within the organization. They help to satisfy customer needs and improve the supply chains of enterprise products. | Customer satisfaction and enterprise services management. | Manages the supply chain of the organization.  Monitor enterprise resources and services. | Decide on marketing strategies.  Decide the best improvements to be actualized in companies for better returns. | Supply chains.  Organization’s marketing mix.  Publicizing organization’s services and applications. | Application’s architect. Organization’s chief marketer. IT Application analyst. |
| Architecture & Infrastructure Committee | It shows the cohesiveness of the organization’s business and information. | Cloud computing entity. | Improve the efficiency of information in the organization.  Rectify functional retardation instances within the organization.  Plan on the best operational motif for other company sectors. | Decide on data consolidation motifs.  Illustrate communication chains to be implemented in the organization. | Organization’s assets accountability. This includes phones, computers, and files.  Client satisfaction plans. | Head of enterprise architecture, System analysts, IT engineers. |
| Enterprise Security Committee | To ensure there are safeguarding paradigms for the organization’s assets, information, and personnel. | Organization’s security and safety department. | Ensure the organization’s information is safe.  Security paradigms for the company’s computers are put safely.  Ensure malicious activities are detected.  Report any system updates to the board for approval. | Decide on security measures to be implemented.  Decide on the security risk management paradigm. | Cybersecurity software, system authentication tools.  Cloud computing technology. | Cloud computing analyst, Business system analyst, Head of networking, Cryptanalysts, Security analysts. |
| Enterprise IT Services Committee | Monitor general services that the company offers. | IT department. Watches out on the general functions that organization offers in relation to technology. | Maintain the best networking services. Ensure there is a monitor on the software services. Embrace the needs that clients have, which includes data security. Communicate service changes in the system. | Decide on the best mode of service delivery.  Makes changes on IT updates and output services nature. | Networking services.  Cloud computing services. | IT manager, IT engineers, Cloud computing officer. |

# **Part B-Charter for the enterprise security committee**

## **Enterprise security committee**

An organization would blossom in its operations when it has a reliable security plan for its clients and employees. Therefore, it needs a committee that helps in ensuring that its data, assets, and employees are safeguarded. Failure in having this committee would yield several negative changes for the organization.

### **Purpose**

The charter is to align the expectations that the organization has from the committees. Having this document helps the committee to perform its functions with ease and benefit from safe dealings (Nagar, 2018). The committee is to purposefully develop and maintain security paradigms set aside to keep assets, information, and the organization’s functions safe.

### **Jurisdiction**

It applies to the security and safety department within the organization.

### **Objectives**

To ensure that the company has a charter and a plan that describes how it will achieve goals that have been set for the company. Besides, it is designed to ensure that the organization archives ultimate security services and better safeguarding motifs for its resources.

### **Responsibilities**

To detect and act upon any malicious activities that the system experiences and any time. Ensures that there are roles accorded to every member of the departments on the mitigations to steps to take in case of security compromise. The committee is on the frontline in creating a risk management plan for the organization to prepare it for the future (Foster, 2020).

### **Decision authority**

Security decisions are made by the panel on what is needed. This includes cryptanalysts, business system analysts, cloud computing management, head of the organization’s security.

### **Membership**

Comprises of cloud computing analysts, head of networking, and security analysts.

### **Deliverables**

Cloud computing technology, cybersecurity software, detectors of malicious objects for individuals visiting the organization.

### **Structure**

Briefings on the organization’s security system are held thrice a week, early in the morning at the boardroom. This involves a report of how every sector is and the various challenges to be addressed.

### **Relationships**

This committee has relationships with individuals from other departments. They are given the authority to watch over other entities within the organization to make every activity safe (Foster, 2020).

### **Executive signatures and dates**

CEO (chairperson) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cloud computing officer\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cryptanalyst \_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security analyst \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Part C:Information Security Policy- IT data classifications**

Policy Written Date： 2021/07/13

Last Revision Date: 2021/07/18

Document Owner: HU ISEM Project Team

|  |  |
| --- | --- |
| Biotech CompanyPolicy and Procedure | |
| Title: Information Security Policy on Data Classification | Policy Number #: BT-IS-DC-1.0 |
| Approval Date: 2021/7/18 | Review: Annual |
| Effective Date: 20121/7/19 | Information Security |

### **Policy Statement**

This policy is to establish Data Classification System to improve the corporate information security in Biotech Company; assist the company in answering crucial data-related issues that influence risk mitigation and data governance rules (Groot, 2021).

### **Purpose**

The purpose of this policy is to establish system on data classification in the proper use of data to meet the current business needs, align with the direction and current stat of the information security program and reduce e the risk mitigation.

### **Scope/Jurisdiction**

This policy document defines information security requirements on Data Classification system that is to create, maintain, store, access, process or transmit information (officeservices, 2020).

Review and oversee the company’s information security and protection on Data Classification, including data access, maintaining regulatory compliance, searchable and retrievable process connected with the company's operation, services, information technology infrastructure, and related operations.

### **Objectives**

The policy is to create a structure and measures of data classification including data categories, workflow creation, identifying classification tools and usage of classified data , have data security regulations in place that employees can adherence to, effectively implement data security and protect the company from the potential security risks (Security Studio, 2020).

### **Definitions**

Data Classification refers to the process of categorizing data into appropriate categories so that it can be used and safeguarded more efficiently. (Groot, 2021)

Data Classification makes data easier to identify and retrieve and is critical to risk management, compliance, and data security (Security Studio, 2020).

### **Policy Requirements & Controls**

The policy requirements defined in this document shall apply to all employees of Biotech company, and must comply with the company IT governance policy.

An access control system will be in place, and unauthorized users must not be allowed to enter or use information resources.

# **References**

CITRIX. (2019, 09 17). *CITRIX SYSTEMS, INC.* Retrieved 07 18, 2021, from CITRIX: https://www.citrix.com/content/dam/citrix/en\_us/documents/about/technology-data-and-information-committee-charter.pdf

Foster, S. (2020). *The Underlying Ideologies of Financial Regulation and Deregulation.* CALIFORNIA LEGAL STUDIES JOURNAL, 32.

Groot, J. D. (2021, 06 17). *DATA PROTECTION 101.* Retrieved 07 18, 2021, from DATAINSIDER: https://digitalguardian.com/blog/what-data-classification-data-classification-definition

Nagar, A. &. (2018). *A semantically rich knowledge representation of PCI DSS for cloud services. .* In 6th International IBM Cloud Academy Conference ICACON 2018, Japan.

officeservices. (2020, 11 20). *Charter: Information Security Committee .* Retrieved 07 18, 2021, from officeservices: https://officeservices.stlawu.edu//charter-information-security-committee

Security Studio. (2020, 01 20). *Information Security Committee Charter, version 1.0.0.* Retrieved 07 18, 2021, from Security Studio: https://securitystudio.com/policy-templates/information-security-committee-charter/