Open Pharma

User Charter

Introduction

OpenPharma is a leading biotech company specializing in pharmaceutical drugs and vaccines. Given the sensitive nature of our work, including valuable intellectual property and patient data, maintaining robust information security is paramount. This User Charter outlines the principles, objectives, and responsibilities that all employees must adhere to, ensuring the confidentiality, integrity, and availability of our information systems.

Principles

- **Confidentiality**: Protecting the confidentiality of our information is paramount. Unauthorized access to sensitive data could lead to financial loss, legal consequences, or damage to our reputation. By restricting access to authorized individuals only, we ensure that our company’s sensitive information remains secure and protected from unauthorized disclosure.
- **Integrity**: We ensure the integrity of our information by implementing measures to prevent unauthorized modifications. Unauthorized changes to data could lead to misinformation, loss of trust from customers or stakeholders, and financial harm. Maintaining data integrity ensures that our information remains accurate, reliable, and trustworthy.
- **Availability**: Our information systems and resources must be available and accessible to you when needed, per our business requirements. Downtime or disruptions in system availability could disrupt business operations, lead to financial losses, or impact our ability to serve customers. By ensuring availability, we maintain business continuity and minimize the risk of disruptions.

Objective

This charter aims to inform all OpenPharma employees of their rights and duties concerning information security, promoting best practices to mitigate risks and protect our organization's assets.

Scope

This charter applies to all employees, contractors, and third-party users who have access to OpenPharma's information systems and data. It encompasses all company-owned or managed data, applications, and IT infrastructure.

User’s Rights and Duties

Information Security Awareness:

Complete mandatory information security awareness training upon joining the company and annually thereafter. This training covers topics such as phishing awareness, password security, and data handling best practices.

Access Control:

Access to company systems and data is granted based on your role and responsibilities. Use unique, strong passwords and enable multi-factor authentication where applicable. Sharing login credentials is strictly prohibited.

Data Handling and Protection:

Handle company data in accordance with its classification level. Sensitive data must be encrypted during storage and transmission. Unauthorized sharing or disclosure of company data is prohibited.

Use of Personal Devices (BYOD Policy):

You may use personal devices for work purposes if they meet the company's security requirements.

Personal devices used for work must have up-to-date antivirus software, be password-protected, and comply with the company's security policies.

incident Reporting:

Promptly report any suspected security incidents, such as phishing attempts, lost devices, or unauthorized access, to the IT security team.

Email and Communication Security:

Be vigilant when handling emails and other communications. Do not open attachments or click on links from unknown or suspicious sources. Verify the authenticity of requests for sensitive information.

Physical Security:

Ensure that physical access to sensitive areas and devices is controlled. Lock your workstation when unattended, and report any unauthorized individuals in secure areas.

Compliance with Legal and Regulatory Requirements:

Adhere to all applicable laws, regulations, and company policies related to information security and data protection. Staying up to date with the latest advancements in biotech and pharmaceutical research.

Checks and Penalties

The IT security team will conduct regular audits and monitoring to ensure compliance with this User Charter and reduce cyber-attacks. Non-compliance may result in disciplinary actions, including revocation of access privileges, mandatory retraining, reduction in bonus pay, or termination of employment, depending on the severity of the breach.

Additional Information

For further guidance or clarification on any aspect of this charter, please contac the IT security team at security@openpharma.com.

Optional - ChatGPT Use

A. Prompts: Help me develop a user chart for employees of a biotech company, focusing on information security principles, user responsibilities, and compliance.

B. Description: I was provided an outline of what I should have in a User Chart. Some of the topics lined up and others did not. I reviewed and customized the output to align with OpenPharma’s specific policies, risks, and organizational context. Additional information from company documents and industry best practices was incorporated to ensure comprehensiveness and compliance measures