Title: Information Security and IT Policy

1. Introduction

This Information Security and IT Policy document outlines the policies and guidelines that all employees, contractors, and vendors of Simpplr must adhere to in order to safeguard the organization's information assets and maintain the privacy and integrity of its IT infrastructure. The policy also addresses compliance with applicable laws and regulations pertaining to information security.

2. Scope

This policy applies to all employees, contractors, and vendors who have access to Simpplr's information assets, including but not limited to computer systems, networks, data, and software. It covers the use of Simpplr-provided and personal devices used for business purposes, as well as any other assets or resources owned or managed by Simpplr.

3. Responsibilities

3.1 Management Responsibilities
The executive management team is responsible for establishing and enforcing information security policies, allocating adequate resources, and providing leadership in ensuring the effectiveness of Simpplr's information security program.

3.2 Employee Responsibilities
All employees are responsible for complying with this policy, protecting information assets, reporting any security incidents or vulnerabilities, and taking necessary precautions to prevent unauthorized access, disclosure, alteration, or destruction of information.

4. Information Security Framework

4.1 Risk Assessment and Management
Simpplr will conduct regular risk assessments to identify and assess risks to its information assets. A risk management process will be implemented to evaluate the impact and likelihood of identified risks and develop appropriate controls and mitigation strategies.

4.2 Information Classification
All information assets owned or managed by Simpplr must be properly classified based on their sensitivity and criticality. Appropriate security controls will be implemented based on the classification level to ensure the confidentiality, integrity, and availability of the information.

4.3 Access Controls
Access to Simpplr's information assets will be granted based on the principle of least privilege, ensuring that employees have access only to the information necessary to perform their job

responsibilities. Strong authentication mechanisms and access control mechanisms will be implemented to protect sensitive information from unauthorized access.

4.4 Data Protection
Simpplr will implement appropriate technical, administrative, and physical controls to protect data from unauthorized access, disclosure, alteration, or destruction. Data encryption, secure backup procedures, and periodic audits will be conducted to ensure data protection.

4.5 Incident Response
An incident response plan will be developed to handle any information security incidents effectively and minimize their impact. This plan will include procedures for reporting incidents, assessing their severity, containing the incident, investigating root causes, and implementing corrective and preventive actions.

4.6 Security Awareness and Training
Simpplr will provide regular security awareness and training programs to ensure that all employees are aware of their responsibilities, understand information security best practices, and are equipped to recognize and respond to security threats.

5. Acceptable Use of IT Resources

5.1 Use of Company IT Resources
Employees are expected to use Simpplr's IT resources for business purposes only. Personal use of these resources should be limited to breaks or when authorized by management.

5.2 Software Usage
Employees must comply with software license agreements, use only authorized software, and refrain from unauthorized installation or distribution of software that may introduce security risks.

5.3 Internet Usage
Simpplr's internet resources must be used responsibly and in compliance with applicable laws and regulations. Employees must avoid accessing, distributing, or transmitting inappropriate, offensive, or illegal material.

6. Policy Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. Simpplr's IT department and management will be responsible for monitoring compliance, investigating violations, and enforcing the policy.

Conclusion

The Information Security and IT Policy is essential for Simpplr to ensure the confidentiality, integrity, and availability of its information assets. Compliance with this policy is mandatory for

everyone associated with the organization. It is the responsibility of every employee, contractor, and vendor to familiarize themselves with this policy and understand their role in protecting Simpplr's information assets and IT infrastructure.