JPCT Company Security Awareness Policy

Introduction:

This document outlines the security policies for employees of JPCT to follow while using company resources and handling sensitive data. Adhering to these policies ensures compliance with industry standards, protection against cybersecurity threats, and the safeguarding of sensitive company and customer data.

Objective:

The objective of this policy is to:

1. Ensure a secure working environment.
2. Educate employees on information security best practices.
3. Provide guidelines for handling company resources and data securely.
4. Mitigate risks of security breaches and data loss.

Sections:

1. Password Management Policy:

• **Password Complexity**: All employees must create strong passwords with a minimum of 12 characters, including uppercase, lowercase, numbers, and special characters.
• **Password Change Frequency**: Employees are required to change their passwords every 90 days to reduce the risk of unauthorized access.
• **Multi-Factor Authentication (MFA)**: Access to sensitive systems must be protected using MFA, requiring at least two verification methods (e.g., password + OTP).

2. Email and Communication Policy:

• **Suspicious Emails**: Employees must not open or respond to suspicious emails. Report any suspicious communication to the IT/security team immediately.
• **Confidential Information**: Avoid sharing sensitive information such as passwords or confidential documents through unsecured channels like public email. Always use encryption when necessary.
• **Phishing Awareness**: Employees must complete phishing awareness training and recognize common signs of phishing attacks (e.g., strange sender addresses, unusual links).

3. Data Protection Policy:

• **Data Encryption**: All sensitive data (e.g., personal, financial, and client information) must

be stored in encrypted formats both in transit and at rest.
• **Access Control**: Access to sensitive documents and systems should be role-based, with permissions granted only to authorized personnel based on the least privilege principle.
• **Data Backup**: Regular backups must be performed for all critical data. Backup systems should also be encrypted to ensure data security.
• **Data Disposal**: When no longer needed, sensitive data must be securely destroyed (e.g., using data wiping or shredding) to prevent unauthorized recovery.

4. Device Usage Policy:

• **Authorized Devices**: Employees are only permitted to access company data and systems from authorized and secured devices. Personal devices are not allowed unless pre-approved by the IT department.
• **Security Software**: All devices must have up-to-date security software, including antivirus programs and firewalls, to protect against malware.
• **Device Loss**: Report any lost or stolen devices to the IT department immediately to ensure access is revoked and data is protected.

5. Public Wi-Fi Usage Policy:

• **Avoid Accessing Sensitive Data on Public Wi-Fi**: Employees should avoid accessing company systems, emails, or confidential data over unsecured public Wi-Fi networks unless connected through a company-provided VPN (Virtual Private Network).
• **VPN Requirement**: Always use a secure VPN connection when accessing company resources remotely to ensure data remains encrypted.

6. Incident Reporting:

• **Reporting Security Incidents**: Any security incident, including data breaches, system compromise, or phishing attempts, must be reported immediately to the IT/security team. Employees must also report any suspicious activity or vulnerabilities they come across in their work environment.
• **Immediate Response**: Employees must not attempt to resolve incidents themselves but rather escalate them promptly through the proper channels for investigation and resolution.
• **Post-Incident Review**: After an incident is resolved, a post-incident review will be conducted to identify lessons learned and improve security measures.

7. Physical Security Policy:

• **Access to Offices**: Physical access to offices and data centers must be controlled through security badges or biometric authentication. Unauthorized personnel must not be allowed to enter restricted areas.

• **Lock Screens**: Employees must ensure that their workstations are locked when left unattended to prevent unauthorized access to sensitive information.
• **Secure Workspace**: Confidential papers should not be left out in the open. All sensitive information must be securely stored in locked cabinets when not in use.

8. Social Engineering Protection Policy:

• **Verifying Identity**: Always verify the identity of callers or visitors who request sensitive information. Do not provide confidential information over the phone or email without proper authentication.
• **Awareness Training**: Employees must undergo social engineering awareness training to identify common tactics used by attackers to manipulate or trick them into revealing confidential data.

9. Social Media Policy:

• **Sharing Company Information**: Employees must not share sensitive company information on social media platforms. This includes but is not limited to client data, project details, or company systems.
• **Use of Personal Social Media**: Personal social media use should not interfere with work activities, and employees should refrain from discussing internal company matters in public forums.

10. Monitoring and Auditing:

• **System Monitoring**: All company systems are monitored for unauthorized access, suspicious activities, and security breaches. Logging and monitoring tools are in place to track all access to sensitive resources.
• **Regular Audits**: Security audits will be conducted regularly to ensure compliance with the policies and procedures. Any findings from audits must be addressed promptly by the responsible teams.

11. Security Awareness Training:

• **Mandatory Training**: All employees are required to complete security awareness training, including phishing simulations, secure password practices, and incident response procedures.
• **Continuous Education**: Employees must participate in ongoing security awareness

programs to stay informed about the latest security threats and best practices.

Conclusion:

Adhering to this Security Awareness Policy is crucial for ensuring that JPCT maintains a high standard of data protection and cybersecurity. Compliance with these policies will help protect both the company and its clients from data breaches, cyber-attacks, and regulatory fines.