Unified Acceptable Use & Information Security Policy

OVERVIEW

This policy outlines the acceptable use of Robotech CAD Solutions' information technology resources and establishes a comprehensive framework for information security. It aims to protect the company's digital assets, ensure compliance with legal and regulatory requirements, and promote a culture of security awareness among all personnel.

SCOPE

This policy applies to all employees, contractors, consultants, temporary workers, vendors, and agents operating on behalf of Robotech CAD Solutions. It encompasses all company-owned or -leased devices, networks, applications, and communication systems.

ACCEPTABLE USE OF IT RESOURCES

- **Ownership and Monitoring**:
  Company-provided systems and networks are the property of Robotech CAD Solutions. Users should have no expectation of privacy; activities may be monitored to ensure compliance.

- **Permitted Use**:
  Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any company policies.

- **Prohibited Activities**:
  - Unauthorized sharing or disclosure of confidential or proprietary information.
  - Installation of unauthorized software or hardware.
  - Use of company resources to engage in illegal, harassing, or offensive conduct.
  - Circumventing user authentication or security controls.
  - Use of pirated or unlicensed software.
  - Sending offensive or disruptive messages, including those with content related to race, gender, age, sexual orientation, religion, or political beliefs.
  - Distributing chain letters, jokes, or unsolicited mass emails.
  - Automatically forwarding company emails to external email systems.
  - Using third-party email services (e.g., Gmail, Yahoo) for conducting company business.

AI TOOL USAGE

- Use of AI tools (e.g., ChatGPT, Bard) with company data must be pre-approved.
- Confidential or proprietary data must not be submitted to AI tools without authorization.

BRING YOUR OWN DEVICE (BYOD)

- Personal devices must be approved by IT prior to accessing company systems.
- Approved devices must run up-to-date security software.

CLOUD STORAGE AND SERVICES

- Use of personal cloud services (e.g., personal Dropbox, Google Drive) for company data is prohibited.
- Only company-approved cloud platforms may be used to store or share company information.

SOCIAL MEDIA AND PUBLIC COMMUNICATION

- Employees may not post or discuss company-related matters on personal social media without approval.
- Confidential or internal information must never be disclosed publicly.

REMOTE WORK AND VPN USAGE

- Remote access must be via company-approved Virtual Private Networks (VPNs).
- Users must ensure secure internet connections and protect company data during remote sessions.

PASSWORD MANAGEMENT

- Passwords must be a minimum of 12 characters and include letters, numbers, and symbols.
- Passwords must be changed every 90 days.
- Use of password managers is encouraged and supported.

SYSTEM INTEGRITY

- Do not disable or circumvent security measures such as antivirus software, firewalls, encryption, or automatic updates installed by the IT team.
- Only use company-approved devices to access work systems.
- Do not install unauthorized software on company devices.

INCIDENT REPORTING

- Report any security breaches, suspicious activities, or mistakes that may compromise security to the Chief Information Officer (CIO) within 60 minutes of discovery.

RESPONSIBLE USE

- Avoid clicking on links from unknown sources or downloading large files from unverified websites.
- Refrain from accessing inappropriate content using company equipment or networks.

SECURITY RESPONSE PLAN (SRP)

- **Development and Maintenance**:
  - Each business unit must develop and maintain a Security Response Plan (SRP) in collaboration with the Information Security (Infosec) team.
  - The SRP should clearly define the services or applications covered, including data flows and system architecture diagrams.
- **Contact Information**:
  - The SRP must include up-to-date contact information for team members responsible for incident response, ensuring availability during non-business hours if necessary.
- **Incident Management**:
  - Define triage procedures to validate and assess reported vulnerabilities or incidents.
  - Outline mitigation strategies and testing procedures prior to deployment.
  - Establish remediation timelines based on the severity and impact of identified vulnerabilities.
- **Compliance and Review**:
  - SRPs must be documented, version-controlled, and reviewed annually.
  - Non-compliance may result in delays in service or product deployment and could lead to disciplinary action.

POLICY COMPLIANCE

- **Monitoring and Auditing**:
  - The Infosec team will conduct periodic audits, system monitoring, and reviews to ensure compliance with this policy.
- **Exceptions**:
  - Any exceptions to this policy must be approved in advance by the Infosec team and documented accordingly.
- **Enforcement**:
  - Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.

ACKNOWLEDGMENT

All employees must read, understand, and sign this Unified Acceptable Use & Information Security Policy upon onboarding and whenever it is updated.