Simply Innovative Unified Communications, LLC

INFORMATION SECURITY POLICY

Effective Date: January 30th 2026
Review Cycle: Annually
Document Owner: Eric C. Berg

1.1 Purpose

This Information Security Policy ("Policy") establishes the framework for protecting the confidentiality, integrity, and availability of information assets owned, processed, or managed by Simply Innovative Unified Communications, LLC ("Company," "we," or "us"). This Policy ensures compliance with applicable legal, regulatory, and contractual obligations while safeguarding customer data, proprietary designs, intellectual property, and business operations.
To establish security standards for protecting company and client data, ensuring compliance with Tennessee state laws (T.C.A. § 47-18-2107) and industry best practices.

1.2 Scope

This Policy applies to:

- All Company personnel, including the owner, employees, contractors, consultants, and temporary staff
- All information assets, including electronic and physical data, systems, networks, devices, and facilities
- All third-party vendors, subcontractors, and partners who access, process, or store Company or customer information
- All remote work environments and cloud-based services utilized by the Company

Applies to all operations of Simply Innovative Unified Communications, focusing on remote engineering and design services.

1.3 Business Context

As a remote-based engineering and design firm specializing in Audio-Visual and Unified Communications solutions, the Company handles sensitive technical designs, customer confidential information, pricing data, project specifications, and proprietary methodologies. Our operations are conducted entirely remotely, and information security is fundamental to maintaining customer trust and competitive advantage.

2.1 Roles and Responsibilities

Owner/Security Officer:

- Establishes and maintains the Information Security Policy
- Ensures adequate resources for security implementation
- Oversees incident response and risk management
- Approves security-related expenditures and vendor relationships
- Conducts annual policy review and updates

All Personnel:

- Understand and comply with this Policy
- Protect Company and customer information assets
- Report security incidents immediately
- Complete required security awareness training
- Use strong authentication and follow access control procedures

Third-Party Vendors/Subcontractors:

- Comply with applicable sections of this Policy
- Maintain their own appropriate security controls
- Execute confidentiality and data protection agreements
- Report security incidents affecting Company or customer data

2.2 Policy Governance

This Policy shall be reviewed and updated annually or when significant business, technological, or regulatory changes occur. All personnel and relevant third parties shall acknowledge receipt and understanding of this Policy.

4.1 User Access Management

- Access to Company systems and customer data shall be granted based on business need and principle of least privilege
- Unique user accounts must be created for each individual; shared accounts are prohibited
- Access rights shall be reviewed quarterly and upon role changes
- Terminated personnel or contractors shall have access revoked immediately upon separation

4.2 Authentication Requirements

- Multi-Factor Authentication (MFA) is required for:
- Password requirements:

4.3 Device Access

- All devices used for Company business (computers, tablets, smartphones) must:

5.1 Data at Rest

- All Confidential Information stored electronically must be encrypted using industry-standard encryption (AES-256 or equivalent)
- Encryption must be applied to:

5.2 Data in Transit

- All Confidential Information transmitted electronically must use secure protocols:

5.3 Data Backup and Recovery

- Critical business data and customer information shall be backed up daily
- Backups must be encrypted and stored securely
- Backup integrity shall be verified monthly
- Disaster recovery procedures shall be tested at least annually
- Backups shall be retained in accordance with legal and contractual requirements

5.4 Data Retention and Disposal

- Customer data shall be retained only as long as necessary for business purposes or as required by contract
- Data no longer required shall be securely deleted or destroyed:

6.1 Network Security

- Firewalls must be enabled on all devices and network equipment
- Wireless networks must use WPA3 or WPA2 encryption at minimum
- Guest networks, if used, must be segregated from business networks
- Remote access to Company systems requires VPN with MFA
- Network security configurations shall be reviewed quarterly

6.2 System Hardening

- All systems and devices must:

6.3 Malware Protection

- Anti-malware software must be installed on all Company devices
- Definitions and signatures must be updated automatically
- Full system scans shall be performed weekly
- Suspicious files or activities must be reported immediately

6.4 Email and Web Security

- Exercise caution with email attachments and links from unknown sources
- Verify sender authenticity before responding to sensitive requests
- Do not click on suspicious links or download unexpected attachments
- Web browsing shall be limited to business-related activities on Company devices
- Secure web gateways or content filtering may be employed to block malicious sites

7.1 Remote Work Environment

Given the Company's remote-only business model:

- Home office networks must be secured with strong passwords and encryption
- Company work must be conducted in a private, secure environment
- Video conferencing and screen sharing must ensure no Confidential Information is visible to unauthorized persons
- Physical documents containing Confidential Information must be stored securely

Use of secure, private Wi-Fi networks only. Use of a VPN is required when accessing client networks or public Wi-Fi.

7.2 Personal Device Use (BYOD)

If personal devices are used for Company business:

- Device must meet minimum security requirements (encryption, password, MFA)
- Company data must be segregated from personal data where possible
- Company reserves the right to remotely wipe Company data if device is lost or stolen
- Personal devices must be disclosed and approved by the Owner

7.3 Public Wi-Fi and Travel

- Public Wi-Fi networks must never be used to access Confidential Information without VPN protection
- Physical security of devices must be maintained while traveling
- Devices must never be left unattended in public spaces
- Sensitive conversations should not be conducted in public where they may be overheard

8.1 Approved Cloud Services

- Only approved cloud services may be used for storing or processing Company or customer data
- Cloud service providers must demonstrate appropriate security controls, including:

8.2 Third-Party Vendor Management

- All vendors and subcontractors with access to Confidential Information must:

8.3 Software as a Service (SaaS) Applications

- SaaS applications must be approved before use for Company business

- MFA must be enabled where available
- Access permissions must be reviewed regularly
- Data must be exportable in the event of service termination

9.1 Incident Reporting

A security incident includes, but is not limited to:

- Unauthorized access to or disclosure of Confidential Information
- Loss or theft of devices containing Company or customer data
- Malware infection or suspected system compromise
- Phishing attacks or social engineering attempts
- Suspected or actual data breaches

All security incidents must be reported immediately to the Owner/Security Officer.

9.2 Incident Response Process

Detection and Reporting:

- Incidents must be reported within 1 hour of discovery
- Do not attempt to investigate or remediate without authorization
- Preserve evidence and logs where possible

In the event of a suspected data breach, the Owner will document the incident immediately.

Assessment and Containment:

- Owner/Security Officer will assess severity and impact
- Immediate containment actions will be taken (e.g., disable accounts, isolate systems)
- Affected customers and relevant parties will be notified as required

Investigation and Remediation:

- Root cause analysis will be conducted
- Vulnerabilities will be remediated
- Systems will be restored from clean backups if necessary

Documentation and Lessons Learned:

- All incidents must be documented, including timeline, impact, and response actions
- Post-incident review will identify improvements to prevent recurrence
- Policy and procedures will be updated as necessary

9.3 Breach Notification

In the event of a data breach involving customer or personal information:

- Affected customers will be notified within 24-72 hours or as required by contract
- Notification will include nature of breach, data affected, and remediation steps
- Regulatory authorities will be notified as required by applicable law
- Legal counsel may be engaged as appropriate

For breaches involving personal information of TN residents or client confidential info, notification will occur within 24 hours of discovery, in alignment with contractual obligations.

10.1 Business Continuity Planning

- Critical business functions and data have been identified
- Alternative work arrangements and backup systems are documented
- Contact information for key personnel, customers, and vendors is maintained
- Business continuity plan is reviewed and tested annually

10.2 Disaster Recovery

- Data backups enable recovery of critical information
- Recovery time objectives (RTO) and recovery point objectives (RPO) are defined for critical systems
- Disaster recovery procedures are documented and accessible
- Systems and data can be restored within 48-72 hours for critical functions

11.1 Home Office Security

- Devices and physical documents must be secured when not in use
- Visitors should not have access to Company devices or Confidential Information
- Physical documents containing Confidential Information must be stored in locked cabinets or secure locations

11.2 Device Security

- Laptops and mobile devices must not be left unattended in vehicles or public places
- Devices must be physically secured with cable locks when used in public spaces
- Lost or stolen devices must be reported immediately for remote wipe capability

12.1 Regulatory Compliance

The Company will maintain compliance with applicable laws and regulations, including but not limited to:

- Tennessee data protection and privacy laws
- Customer contractual security requirements
- Industry-specific regulations applicable to our customers (e.g., HIPAA for healthcare, FERPA for education)
- Federal information security standards where applicable

12.2 Contractual Obligations

- Customer contracts and master agreements will be reviewed for security requirements
- Security controls will be implemented to meet or exceed customer requirements
- Evidence of compliance will be provided upon customer request (e.g., insurance certificates, policy documentation)

12.3 Intellectual Property Protection

- Company proprietary methodologies, designs, and trade secrets are protected as Confidential Information
- Customer intellectual property and proprietary information is protected in accordance with contract terms
- Copyright and licensing requirements for third-party software and materials are respected

13.1 Training Requirements

All personnel must complete security awareness training:

- Upon hire or engagement
- Annually thereafter

- When significant policy changes occur

Training topics include:

- Information security policies and procedures
- Phishing and social engineering awareness
- Password security and MFA usage
- Incident reporting procedures
- Data handling and classification
- Remote work security best practices

13.2 Security Communications

- Security alerts and updates will be communicated promptly
- Personnel are encouraged to ask questions regarding security practices
- Security is a shared responsibility across all Company activities

14.1 Acceptable Use of Company Resources

Company information systems and devices are provided for business purposes. Acceptable use includes:

- Conducting Company business and customer engagements
- Communication with customers, vendors, and business partners
- Professional development and industry research
- Incidental personal use that does not interfere with business operations or violate this Policy

14.2 Prohibited Activities

The following activities are strictly prohibited:

- Accessing, storing, or transmitting illegal, offensive, or inappropriate content
- Unauthorized access to systems, networks, or data
- Attempting to bypass security controls
- Installing unauthorized software or hardware
- Sharing authentication credentials
- Using Company resources for personal commercial activities
- Engaging in activities that could damage Company reputation
- Violating intellectual property rights or software licensing agreements

14.3 Monitoring and Privacy

- The Company reserves the right to monitor use of Company systems and devices to ensure compliance and security
- Personnel should have no expectation of privacy when using Company resources
- Monitoring will be conducted in accordance with applicable laws

15.1 Compliance Monitoring

- Compliance with this Policy will be monitored through periodic reviews and audits
- Security metrics and key performance indicators will be tracked
- Vulnerabilities and non-compliance issues will be documented and remediated

15.2 Violations and Consequences

Violations of this Policy may result in:

- Verbal or written warning
- Suspension of access to Company systems

- Termination of employment or contract
- Legal action where appropriate
- Reporting to law enforcement for criminal violations

15.3 Exceptions and Waivers

- Exceptions to this Policy require written approval from the Owner/Security Officer
- Exceptions will be documented with business justification and compensating controls
- Exceptions will be reviewed quarterly and reauthorized or revoked as appropriate

This Policy shall be reviewed at least annually and updated as necessary to reflect:

- Changes in business operations or services
- New technologies or security threats
- Customer requirements or contractual obligations
- Regulatory or legal changes
- Lessons learned from security incidents

16.1 Document Control Log

Version	Time period	Approved By:	Title	Notes
1.0	February 2024 – January 2025	Eric C. Berg	Owner	Original
1.1	January 2025 – February 2026	Eric C. Berg	Owner	Added: Third-Party Vendor Management Updated: 9.1-9.3
1.2	February 2026 - January 2027	Eric C. Berg	Owner	No changes made