VoIP Security Policy Document

Date: Thursday 12th June 2026

Prepared by: Group 8 Security Team[G8ST]

1. Introduction

Voice over Internet Protocol (VoIP) technology has revolutionized enterprise communication by enabling cost-effective, flexible, and feature-rich voice services. However, due to its dependence on IP-based networks, VoIP is susceptible to various cybersecurity threats, including eavesdropping, call hijacking, spam over Internet telephony (SPIT), denial-of-service (DoS) attacks, and voice phishing (vishing).

This VoIP Security Policy outlines the minimum security standards and practices that must be followed to ensure the confidentiality, integrity, and availability of voice communication services deployed across G8ST's infrastructure. VoIP is a core element of our digital communication strategy, and its security is critical to the protection of sensitive business conversations, client information, and internal coordination across all departments.

The evolution of cyber threats in recent years, particularly the increase in protocol-specific attacks, has made it essential for organizations to approach VoIP with a rigorous, layered security model. This policy also aligns with international best practices such as the NIST Cybersecurity Framework, ISO/IEC 27001 standards, and the General Data Protection Regulation (GDPR) for secure handling of personally identifiable information during VoIP transmission.

2. Purpose

The purpose of this policy is to:

- Define standardized VoIP system security requirements for the enterprise.
- Provide a structured framework for encryption, authentication, access control, and monitoring.
- Mitigate risks associated with unauthorized access, call interception, fraud, and service disruptions.

- Promote a culture of cybersecurity awareness specific to voice communication technologies.
- Establish accountability among stakeholders and enforce compliance through regular audits and reviews.

In addition to enhancing operational security, this policy aims to support organizational resilience by ensuring VoIP communication remains available during emergencies or system failures, and that backup and recovery processes are clearly defined and tested.

3. Scope

This policy applies to all individuals and entities within G8ST, including:

- Full-time and part-time employees
- Contractors and consultants
- Vendors and third-party service providers with VoIP access
- All branches, satellite offices, and remote users who utilize corporate VoIP systems

It also covers:

- VoIP telephony infrastructure including Asterisk PBXs, IP phones, softphones, SIP trunks, SBCs, routers, and firewalls
- On-premise, cloud-hosted, and hybrid VoIP deployment models
- Communication channels integrating VoIP features such as video calls, voicemail, conferencing, and fax-over-IP (FoIP)

This scope includes initial VoIP implementation, ongoing operation, upgrades, and decommissioning of systems.

4. Roles and Responsibilities

A secure VoIP environment is a shared responsibility requiring collaboration among various stakeholders.

IT Security Team:

- Define and enforce VoIP-specific security controls.
- Configure firewalls, IDS/IPS systems, and encryption protocols.
- Monitor logs and conduct regular penetration tests.
- Provide cybersecurity training and awareness specific to VoIP threats.

System Administrators:

- Maintain VoIP servers, apply firmware updates, and patch vulnerabilities.
- Implement secure call routing policies.
- Control access privileges based on user roles.
- Document all configurations and system changes in compliance logs.

VoIP Service Providers:

- Ensure the security of SIP trunks and hosted services.
- Cooperate during incident response and compliance audits.
- Adhere to Service Level Agreements (SLAs) that include security metrics.

Employees and End Users:

- Use approved VoIP applications and strong SIP credentials.
- Report anomalies or security incidents related to voice calls.
- Avoid using personal devices without approval.
- Follow the VoIP Acceptable Use Policy (AUP).

5. VoIP System Security Standards

Security standards are grouped into categories for easier implementation and tracking.

5.1 Authentication & Access Control

- Unique usernames and strong passwords must be enforced for all SIP accounts.
- Passwords must be at least 12 characters long and contain uppercase, lowercase, numbers, and symbols.
- Default passwords must be changed during initial configuration.
- SIP accounts must be deactivated immediately upon user termination.

- VoIP admin interfaces (e.g., Asterisk Web UI) must be protected by multi-factor authentication (MFA).
- Session timeouts must be configured to automatically log out inactive users.

5.2 Encryption Requirements

- TLS must be enabled to protect SIP signaling.
- SRTP must be enforced for media encryption.
- VoIP systems must use modern ciphers (AES-256 or higher) and reject deprecated protocols (e.g., SSLv3).
- Certificates must be managed through a Public Key Infrastructure (PKI) and renewed before expiration.
- Secure VPN tunnels must be used for remote access to internal VoIP systems.

5.3 Network Segmentation

- VoIP traffic must be segregated using dedicated VLANs.
- Management traffic, such as provisioning and firmware updates, must be on separate secure channels.
- Guest access networks must be isolated from VoIP VLANs.
- Firewalls must inspect SIP and RTP traffic using SIP-aware modules (ALG disabled if necessary).

5.4 Device Hardening

- Disable unnecessary services and ports on VoIP devices.
- Lock IP phones to restrict local configuration changes.
- Disable web interfaces on IP phones unless required.
- Enable tamper detection features where available.
- Periodically audit device configurations and logs.

5.5 Intrusion Detection & Monitoring

- Deploy VoIP-aware IDS such as Snort or Suricata.
- Custom SIP rules must detect INVITE floods, SIP fuzzing, and REGISTER scans.
- Logs must be collected centrally and reviewed daily.
- All VoIP systems must be integrated into the corporate SIEM.
- Suspicious activity must trigger real-time alerts to the security operations center.

5.6 Software and Firmware Maintenance

- Firmware updates must be scheduled and tested in staging environments before production rollout.
- Auto-update settings must be enabled where safe.
- Unsupported devices must be retired according to asset lifecycle policies.
- Patch management must include VoIP operating systems and third-party applications.

5.7 Fraud and Abuse Prevention

- Toll fraud prevention rules must restrict international calling by default.
- Call patterns must be monitored for anomalies using behavioral analytics.
- Daily call limits and thresholds must be configured to detect abuse.
- Long-duration calls should be flagged and manually verified.

6. BYOD (Bring Your Own Device) Policy

To support flexible work environments while maintaining security:

- ➢ Only IT-vetted apps (Zoiper) are permitted.
- ➢ Personal devices must meet baseline security standards (e.g., OS version, lock screen).
- ➢ Access must be via secure VPN.
- ➢ Corporate VoIP accounts must be deprovisioned upon exit or contract completion.
- ➢ IT has the right to remotely wipe VoIP-related data from BYODs during an incident.
- ➢ BYOD users must complete mandatory VoIP security orientation.

7. Incident Response Protocol

Incident handling procedures must ensure rapid mitigation of any VoIP-related breach.

7.1 Detection

- Triggered by IDS/IPS alerts, user reports, or abnormal traffic patterns.
- Examples include:
  - Brute-force SIP login attempts

    - Sudden surge in call volume
    - Unauthorized geographic SIP registrations

7.2 Containment

- Block source IP at firewall level.
- Disable affected SIP account.
- Isolate compromised systems.

7.3 Investigation

- Review call detail records (CDRs), system logs, and packet captures.
- Determine scope and origin of attack.

7.4 Recovery

- Reset credentials and reconfigure devices.
- Verify all security controls are restored.
- Resume normal operation after validation.

7.5 Post-Incident Activities

- Conduct a postmortem.
- Document findings and update response plan.
- Train staff if social engineering was involved.

8. VoIP User Awareness Guidelines

Security begins with informed users. All staff should:

- Be aware of SPIT and phishing through VoIP.
- Avoid clicking links in voicemail-to-email transcriptions.
- Use headsets and avoid speakerphones in shared environments.
- Lock devices after use.
- Report all strange call behavior to the helpdesk.

Regular reminders, posters, and emails will be used to promote best practices.

9. Audit and Compliance

- Internal audits will be conducted quarterly.
- External audits must be performed annually.
- VoIP systems will be assessed against a hardening checklist.
- Logs must be retained for at least 180 days.
- Non-compliance must be remediated within 15 days of discovery.
- Reports are filed with the IT Governance Board.

10. Policy Review and Maintenance

- The policy must be reviewed at least once every 12 months.
- Major updates require formal approval and training dissemination.
- All staff will be notified of significant changes.
- Archived versions of the policy will be retained for 5 years.

Approval:

Name: __G8ST Management______
Title: _______________________
Signature: ____________________
Date: __ 12TH June 2025_________