UNIVERSITY OF BUEA

FACULTY OF ENGINEERING AND TECHNOLOGY

Department of Computer Engineering

CEF 458:

ENTERPRISE IP (VoIP) AND TELEPHONY NETWORKS

Group 8 SECURITY TEAM – PROJECT

Organizational VoIP Security Policy and Awareness Toolkit

GROUP H MEMBERS	MATRICULE
FOMECHE ABONGACHU SIDNEY	FE22A218
EPANDA RICHARD JUNIOR	FE22A206

CONTENTS

CHAPTER 1

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_________

CHAPTER 2

VoIP Security awareness Training Slides and Frequently Asked Questions (FAQ)

1. What is VoIP and why does it need special security?

VoIP (Voice over IP) lets you make voice calls over the internet. Because it runs on IP networks, it's exposed to the same risks as web servers—hacking, eavesdropping, and phishing.

2. What is SPIT and how do I avoid it?

SPIT = Spam over Internet Telephony. These are unwanted or fake calls meant to trick you.

✓ Never answer unknown or suspicious numbers.

✓ Don’t share personal info over unsolicited calls.

3. What should I do if a caller asks for my extension password?

Hang up immediately. No real IT or admin team will ask you for your credentials over the phone.

4. Is it safe to use my personal phone for VoIP calls?

Only if it's approved and configured by IT. Always use the company-recommended apps like Zoiper or Linphone and connect via VPN.

5. How do I report strange call behavior?

If you receive repeated spam calls, unusual call logs, or poor audio quality, contact the IT Helpdesk immediately with as much detail as possible.

USER AWARENESS GUIDE

Title: “Think Before You Speak – Stay Safe on VoIP!”

Phishing Over VoIP (Vishing)

- Attackers impersonate support teams or admins.
- They ask for passwords, codes, or system access.
- **Don’t trust unfamiliar voices — verify through official channels.**

SPIT – Spam Over Internet Telephony

- You may receive calls that play fake promotions or ask you to press numbers.
- **Do not interact with the keypad. Hang up and report.**

Social Engineering

- Hackers gather personal info from social media or previous calls.
- Then they call you pretending to know your team or manager.
- **Never reveal internal processes or access instructions over the phone.**

How to Stay Safe:

- Use strong SIP passwords.
- Never reuse extension passwords across services.
- Always lock your devices when away.
- Avoid taking VoIP calls on public Wi-Fi.
- Keep your softphone apps and OS updated.
- Report anything weird. Fast.
-

Appendix:

Powerpoint slides on the Repository: *https://github.com/Sidney-Fomeche/GROUP8*

CHAPTER 3

Group H Security Team VoIP Incident Response Checklist

Date: Thursday 12th June 2025

Prepared by: Group H Security Team

1. Purpose

This playbook outlines the standardized procedures to detect, assess, contain, respond to, and recover from security incidents involving Voice over IP (VoIP) systems within the organization. It is designed to assist the Group H Security Team in ensuring prompt and effective handling of VoIP-related threats to protect confidentiality, integrity, and availability.

2. Scope

Applies to all VoIP communication systems, including but not limited to: - Asterisk servers - IP desk phones and softphones - SIP and RTP traffic - Session Border Controllers (SBCs) - Remote and mobile VoIP users

3. Roles and Responsibilities

Role	Responsibility
Incident Manager	Oversees response process and reporting
VoIP Engineer	Performs technical containment and restoration
Security Analyst	Conducts investigation and analysis
Communication Lead	Coordinates internal and external communications
IT Support	Assists in recovery and user notification

4. Incident Categories

Category	Description
Unauthorized Access	Use of stolen SIP credentials, unauthorized device registration
SPIT (VoIP Spam)	Mass unsolicited calls disrupting business functions
Call Interception	Eavesdropping or audio stream capture
Denial of Service (DoS)	SIP flooding, RTP disruption, or server overload
Configuration Breach	Misconfigurations leading to vulnerability exposure

5. Incident Response Lifecycle

5.1 Identification & Detection

- Continuous monitoring with IDS (Snort/Suricata) and VoIP logs
- Alerts for:
  - Multiple failed SIP REGISTER attempts
  - Sudden spike in INVITE messages
  - Abnormal call duration or destination
- Initial triage using SIEM alerts and correlation rules

5.2 Reporting & Notification

- Internal users report incidents via helpdesk or hotline
- IDS alert escalates to the Security Analyst
- Incident Manager initiates incident ticket and assigns roles
- Notify stakeholders and legal counsel if sensitive data is impacted

5.3 Containment

- Immediate actions:
  - Block offending IP via firewall
  - Suspend compromised SIP accounts
  - Isolate affected VoIP segment or VLAN
- Short-term measures:
  - Rate-limit SIP traffic

  - Disable auto-provisioning on exposed phones

5.4 Investigation & Analysis

- Collect:
  - Asterisk logs, call detail records (CDRs)
  - Packet captures (PCAPs) from SPAN port or IDS
  - Authentication logs, extension activity
- Analyze:
  - Root cause (vulnerability exploited, attacker IP, breach vector)
  - Lateral movement (other extensions affected?)

5.5 Eradication & Recovery

- Remove malicious IPs and sessions
- Patch vulnerable components
- Reset passwords and regenerate SIP secrets
- Restore services and test call integrity
- Verify TLS/SRTP is functioning and trusted certificates are in place

5.6 Communication & Documentation

- Prepare executive summary of incident
- Notify all affected users with instructions
- Document timelines, actions taken, tools used
- Maintain incident records in centralized system

5.7 Post-Incident Review

- Conduct review within 5 business days
- Identify gaps in detection or response
- Recommend improvements (e.g., new Snort rules, better monitoring)
- Update this playbook if necessary

6. Communication Plan

Audience	Method	Frequency	Responsible
Affected Users	Email	Once confirmed	IT Support
Executives	Report	Within 24h	Incident Manager
External Vendors	Phone/Email	If needed	Communication Lead

7. Tools and Resources

- IDS/IPS: Snort, Suricata
- Packet Capture: Wireshark
- SIEM Platform:[log manager]
- VoIP Server: Asterisk CLI, log monitoring tools
- VPN and Firewall: pfSense or equivalent
- Communication: Internal ticketing system, Slack, Email

8. Review and Maintenance

- The playbook must be reviewed annually or after every major incident.
- Changes require approval from the Head of Security.
- Latest version must be stored in the organization’s security document repository.

Approval:
Name: __G8ST Management______
Title: ________________________
Signature: _____________________
Date: __ 12TH June 2025_________

CHAPTER 4

Audit-Friendly VoIP Deployment Hardening Checklist

Date: Thursday 12th June 2024

Prepared by: Group 8 Security Team [G8ST]

Purpose

This checklist is designed to assist audit teams and system administrators in verifying the secure configuration and deployment of Voice over IP (VoIP) systems. It ensures alignment with industry standards and internal VoIP security policies.

Instructions

- Use this checklist before system go-live, quarterly audits, and after significant configuration changes.
- Mark each item as **Compliant (✔)**, **Non-Compliant (✘)**, or **Not Applicable (N/A)**.
- Record additional notes or observations where relevant.

VoIP Deployment Hardening Checklist

#	Checklist Item	Compliance	Notes
1	SIP signaling is encrypted using TLS		
2	RTP media streams are encrypted using SRTP		
3	Strong, complex SIP passwords are enforced for all users		
4	Default VoIP account credentials have been changed		
5	Asterisk/VoIP server access is restricted to authorized IP addresses		

#	Checklist Item	Compliance	Notes
6	Admin interfaces (AMI, web GUIs) are protected behind VPN or firewall		
7	All VoIP system software and firmware are up to date		
8	Unused SIP extensions, ports, and services are disabled		
9	IP phones are segmented via VLANs separate from data traffic		
10	QoS (Quality of Service) is configured to prioritize VoIP traffic		
11	Fail2Ban or equivalent is configured for brute-force SIP login attempts		
12	Snort/Suricata IDS rules for VoIP threats are enabled and tuned		
13	VoIP logs are centralized and stored for a minimum of 90 days		
14	Softphones are restricted to authorized apps (e.g., Zoiper, Linphone)		
15	VoIP system access via mobile devices requires VPN connection		
16	BYOD usage is governed by policy and devices are registered		
17	Rate limiting is enabled on SIP traffic to prevent DoS attacks		
18	Call Detail Records (CDRs) are retained for forensic review		
19	TLS certificates are valid and issued by trusted authorities		
20	SNMP and remote access services are disabled unless required		
21	Regular vulnerability scans are conducted on VoIP infrastructure		

#	Checklist Item	Compliance	Notes
22	Multi-factor authentication (MFA) is implemented for admin access		
23	Auto-provisioning of IP phones is secured and access-controlled		
24	Password policies enforce expiration, reuse prevention, and complexity		
25	VoIP system documentation and configurations are backed up securely		

Review & Sign-Off

This checklist must be reviewed and signed off by the designated VoIP Security Lead during each audit cycle.

Security Lead Name: G8ST
Title: ___Compliance Form_________
Signature: ________________________
Date: __________________________

Retention: Store a signed copy of each completed checklist for at least three years in the compliance audit archive.

Conclusion

The Group 8 Security Team has developed a comprehensive VoIP Security Documentation Toolkit that addresses the critical need for secure, resilient, and user-conscious voice communication systems within modern enterprise environments.

Through a multi-layered approach covering policy enforcement, technical hardening, incident response, and user awareness, this project demonstrates a robust understanding of the threats that VoIP systems face and the best practices necessary to mitigate them. Our deliverables include a detailed VoIP Security Policy, an audit-ready Deployment Hardening Checklist, an actionable Incident Response Playbook, and a creative Awareness Toolkit designed to empower end-users against SPIT, phishing, and social engineering attacks.

Each component of this project was curated to align with international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework, ensuring not only academic excellence but also real-world applicability in enterprise and telecommunication environments.

We believe that this project reflects our technical knowledge, strategic thinking, and readiness to address evolving security demands in IP-based communication networks. It also reinforces the importance of both infrastructure resilience and human vigilance in achieving true security.

Group 8 Security Team is proud to submit this work as a benchmark for enterprise-grade VoIP security planning and execution.