

FRAUD & SECURITY POLICY

Firstcom Europe Ltd Version: 2026.1 — Effective from: 01/08/2026

This Fraud & Security Policy (“Policy”) forms part of the Agreement between Firstcom Europe Ltd (“Firstcom”) and the Customer. Its purpose is to protect both parties from telecoms fraud, cyber-security threats, and misuse of services.

1. PURPOSE OF THIS POLICY

This Policy sets out:

- The Customer’s responsibilities for securing their systems
- Firstcom’s monitoring and protective measures
- What happens if fraud or suspected fraud occurs
- Liability boundaries and cost responsibility
- Emergency suspension rules

This Policy applies to all telecoms, hosted voice, SIP, connectivity, and IT services provided by Firstcom.

2. DEFINITIONS

- **Fraud:** Any unauthorised, unlawful, or malicious use of telecoms or IT services resulting in financial loss or security compromise.
- **Toll Fraud:** Unauthorised access to a PBX, handset, router, or system resulting in outbound calls being made without permission.
- **Security Compromise:** Any event where systems, credentials, or devices are accessed or controlled by unauthorised parties.
- **AGT (Artificially Generated Traffic):** Automated or manipulated call traffic not originating from genuine human use.

3. CUSTOMER RESPONSIBILITIES

The Customer is responsible for securing all equipment, systems, and credentials under their control, including:

- PBX systems (on-premise or hosted)
- Handsets, softphones, and mobile devices
- Routers, firewalls, and network equipment
- Wi-Fi networks and access points
- Administrator passwords and user accounts

The Customer must:

- Maintain strong, unique passwords
- Restrict remote access to authorised personnel
- Keep systems patched and updated
- Ensure SIP ports are secured or restricted
- Disable unused extensions, call forwarding, or voicemail-to-external features
- Notify Firstcom immediately of any suspected compromise

Failure to secure equipment may result in financial liability for fraudulent usage.

4. FIRSTCOM RESPONSIBILITIES

Firstcom will:

- Monitor network traffic for signs of fraud
- Apply fraud-prevention tools where available
- Notify the Customer promptly if suspicious activity is detected
- Provide guidance on securing systems
- Take reasonable steps to minimise further loss once notified

Firstcom does **not** guarantee prevention of all fraud, as many attacks originate from vulnerabilities within Customer-controlled systems.

5. TOLL FRAUD & UNAUTHORISED CALLS

The Customer acknowledges that:

- Toll fraud is a known industry risk
- Most toll fraud originates from insecure PBX systems, weak passwords, or exposed SIP ports
- The Customer is responsible for securing their own equipment

5.1 Liability for Fraudulent Calls

Unless expressly stated otherwise in writing:

- The Customer is liable for all call charges incurred on their service, **including fraudulent or unauthorised calls**
- Firstcom is not responsible for costs arising from insecure Customer equipment
- Firstcom may, at its discretion, apply temporary call barring to limit further loss

6. FRAUD DETECTION & EMERGENCY ACTION

If Firstcom detects or suspects fraud, it may take immediate action, including:

- Blocking outbound calls
- Restricting international or premium destinations
- Suspending SIP or hosted voice services
- Applying rate limits or call caps
- Contacting the Customer's authorised contact

These actions are taken to protect the Customer from further financial loss.

7. CALL BARRING & SPEND LIMITS

Firstcom may apply:

- Daily or monthly spend limits
- Destination-based restrictions
- International call barring
- Premium rate blocking

The Customer may request changes to these controls, but doing so may increase fraud risk.

8. SECURITY BEST PRACTICES

The Customer must follow industry-standard security practices, including:

- Using complex passwords (minimum 10 characters, mixed type)
- Changing default credentials on all devices
- Restricting SIP access to known IP addresses
- Using VPNs for remote access
- Enabling two-factor authentication where available
- Disabling international dialling if not required
- Regularly reviewing call logs for anomalies

9. CONNECTIVITY & NETWORK SECURITY

For broadband, FTTP, SoGEA, and Ethernet services, the Customer must:

- Secure routers and firewalls
- Disable remote management unless required
- Protect Wi-Fi with WPA2/WPA3 encryption
- Prevent unauthorised access to LAN devices

Firstcom is not responsible for breaches caused by insecure Customer networks.

10. INCIDENT REPORTING

The Customer must report suspected fraud immediately via:

- Email: [Insert Support Email]
- Telephone: [Insert Support Number]

Firstcom will investigate and take reasonable steps to mitigate further loss.

11. COST RESPONSIBILITY

Unless otherwise agreed:

- The Customer is responsible for all fraudulent call charges
- Firstcom may invoice charges incurred prior to detection
- Firstcom is not liable for consequential loss arising from fraud

12. POLICY UPDATES

Firstcom may update this Policy to reflect:

- New fraud risks
- Regulatory changes
- Network improvements
- Industry best practice

Updated versions will be published or provided to the Customer.

END OF FRAUD & SECURITY POLICY