Advocacy Center
for Democratic Culture

INTERNET CYBERSECURITY PRACTICES AND DIGITAL SAFETY PROCEDURES

Adopted: 2026
Applies to: All staff, consultants, volunteers and external collaborators

www.acdc-kosovo.org

1. Purpose and Scope

This document defines the internal cybersecurity standards, digital safety rules, and data protection mechanisms of ACDC. Its primary objective is to ensure the protection of sensitive organizational data, donor information, beneficiary records, financial documentation, and communication systems.

The policy establishes preventive measures against cyber threats such as phishing, hacking attempts, malware infections, social engineering, identity theft, and unauthorized access to digital platforms.

These procedures apply to all ACDC offices (North Mitrovica, Prishtina, Belgrade), including all official devices, servers, cloud services, websites, social media platforms, internal databases, and communication tools used for professional purposes.

2. Identified Risks and Organizational Response

Following internal assessments and previous cyber incidents, including the breach of official social media accounts, ACDC identified several structural and operational vulnerabilities. These included unstable internet routing, lack of centralized data storage, insufficient multi-factor authentication, and limited structured cybersecurity awareness among staff.

In response, ACDC implemented comprehensive corrective measures including:

- Adoption of Starlink as official internet provider to ensure stable, secure connectivity.
- Introduction of official Meta Business profiles with controlled administrative access.
- Installation of a centralized internal server for secure document management.
- Implementation of antivirus software across all official devices.
- Mandatory staff cybersecurity training sessions.
- Introduction of internal incident response protocols.

These measures significantly reduce operational risk and enhance digital resilience.

3. Internet and Network Security

ACDC uses Starlink as its official internet service provider to ensure stable, encrypted, and reliable internet access. The network infrastructure is password-protected and access credentials are restricted to authorized technical staff only.

The organization applies the following network security standards:

- Strong router-level password encryption.
- Periodic password changes.
- Separation of internal network and guest access (where applicable).
- Restricted remote access permissions.
- Monitoring of unusual network activity.

Unauthorized installation of network equipment or sharing of network credentials is strictly prohibited.

4. Centralized Server and Data Management

ACDC has implemented a centralized internal server to regulate file storage, reduce reliance on external file transfers, and ensure structured document management.

The server provides:

- Controlled access based on staff roles.
- Secure storage of financial, legal, and programmatic documentation.
- Reduced dependency on personal devices for document sharing.
- Organized data architecture to prevent duplication and data loss.

Regular backups are conducted and stored in protected environments. Cloud services used by ACDC are protected by two-factor authentication and access control procedures. Access rights are revoked immediately upon termination of employment or consultancy.

5. Device Security

All official laptops and office computers are equipped with licensed antivirus software (e.g., NOD32 or equivalent). Automatic security updates are enabled to ensure protection against emerging threats.

Device usage standards include:

- Mandatory password protection on all devices.
- Automatic screen lock after inactivity.
- Prohibition of installing unauthorized software.
- Prohibition of using public computers for official account access.
- Secure storage of devices when not in use.

USB devices and external drives must be scanned before use. Lost or stolen devices must be reported immediately.

6. Social Media and Online Presence Protection

After experiencing unauthorized access to social media accounts, ACDC strengthened its digital platform governance. Measures include:

- Use of official Meta Business Suite accounts only
- Mandatory two-factor authentication on all social media platforms.
- Role-based administrative access (Primary: Communication Officer; Backup: Executive Director)
- Immediate removal of access for former staff members.
- Secure password storage using password management tools.

Only designated staff are authorized to publish or manage official content.

7. Email and Communication Security

All official communication must be conducted through @acdc-kosovo.org email accounts.
Staff are trained to recognize phishing emails, suspicious attachments, and malicious links.

Security procedures include:

- Prohibition of downloading unknown attachments.
- Verification of suspicious emails with sender via alternative communication channel.
- Immediate reporting of potential phishing attempts.
- Regular password updates and 2FA activation.

Confidential donor and beneficiary data must never be shared via unsecured messaging applications.

8. Staff Capacity Building and Awareness

Recognizing that human error is a primary cybersecurity vulnerability, ACDC organizes structured training sessions to enhance staff awareness of digital risks.

Training topics include:

- Identification of phishing attempts and malicious websites.
- Safe browsing and password management practices.
- Secure handling of sensitive data.
- Digital hygiene and privacy standards.
- Responsible and ethical use of Artificial Intelligence tools.

Cybersecurity orientation is included in onboarding procedures for new staff and volunteers.

9. Password Policy

ACDC enforces strong password standards:

- Minimum 12 characters.
- Combination of uppercase, lowercase, numbers, and special characters.
- No password reuse across platforms.
- Use of password managers recommended.
- Passwords must not be shared via email or messaging apps.

Periodic password changes are mandatory for high-level administrative accounts.

10. Incident Response Procedure

In case of suspected cybersecurity incident, the following steps must be taken immediately:

1. Disconnect affected device from internet.
2. Notify Executive Director and Communication Officer.
3. Change compromised passwords.
4. Document incident details.
5. Inform relevant partners/donors if necessary.
6. Restore systems from secure backups if required.

A post-incident review is conducted to assess root causes and prevent recurrence.

11. Data Protection and Confidentiality

ACDC handles sensitive personal, financial, and legal data with strict confidentiality.

Measures include:

- Restricted access to personal beneficiary data.
- Secure storage of legal documentation.
- Non-disclosure obligations for staff and consultants.
- Controlled sharing of financial information.
- Compliance with applicable data protection principles

Sensitive information must not be stored on personal devices without authorization.

12. Monitoring and Review

This cybersecurity policy is reviewed annually and updated in line with technological advancements and organizational growth. Cybersecurity improvements are integrated into ACDC's 2026–2030 strategic framework, ensuring long-term digital resilience and crisis preparedness.

13. Compliance

All staff, consultants, and volunteers are required to comply with this policy. Failure to adhere to cybersecurity standards may result in internal disciplinary measures. The Executive Director and Program Management oversee policy implementation and enforcement.

www.acdc-kosovo.org
office@acdc-kosovo.org
www.facebook.com/Ngoacdc
www.instagram.com/acdc.kosovo
www.x.com/ngo_acdc