BALKANS
FORWARD
FOUNDATION

DIGITAL AND INFORMATION SECURITY POLICY

Balkans Forward Foundation

DIGITAL AND INFORMATION SECURITY POLICY

Table of Contents

1. Purpose

The purpose of this Digital and Information Security Policy is to ensure that Balkans Forward Foundation ("the Foundation") protects its digital systems, devices, accounts, communications, files, and sensitive information against unauthorised access, misuse, loss, damage, disclosure, or disruption.

The Foundation recognises that information security is essential to organisational integrity, continuity of work, protection of partners and participants, and safeguarding of sensitive human rights-related information.

2. Scope

This policy applies to all digital systems, devices, accounts, files, communication tools, platforms, and information used, accessed, stored, or managed by or on behalf of the Foundation.

It applies to all persons acting on behalf of the Foundation, including the Founder, Board members, Executive Director, staff, consultants, interns, volunteers, external experts, and other authorised persons.

It applies to both Foundation-owned and personally used devices where they are used for Foundation work.

3. General Principles

All persons handling Foundation information or using Foundation systems must do so responsibly, securely, and in a way that minimises risk.

Security measures must be proportionate to the sensitivity of the information, the level of risk, and the operational realities of the Foundation.

Information must be protected against unauthorised access, accidental loss, theft, damage, or inappropriate disclosure.

4. Access and Account Security

Access to systems, platforms, files, and accounts must be limited to authorised persons only and only to the extent necessary for their role.

Strong and unique passwords must be used for Foundation-related accounts and systems.

Where available, multi-factor authentication should be enabled for email, cloud storage, financial systems, communication tools, and other important accounts.

Accounts, passwords, or access credentials must not be shared unless strictly necessary and appropriately managed.

Access should be removed or updated promptly when roles change or engagements end.

5. Devices and Physical Security

Laptops, phones, storage devices, and other equipment used for Foundation work must be kept secure and protected from theft, loss, or unauthorised access.

Devices should be protected by passwords, PINs, biometric protection, or other appropriate access controls.

Where reasonably possible, devices should use updated software, operating systems, and security protections.

Users must take appropriate care when working in public spaces, travelling, or handling sensitive information outside secure environments.

6. Storage, Backup, and File Management

Foundation files and information should be stored in organised, secure, and appropriate locations.

Important documents should not be stored only on personal devices where this creates risk of loss or inaccessibility.

Where relevant and feasible, backup arrangements should be used to reduce the risk of data loss.

Shared folders, cloud storage, and collaborative tools should be structured to protect confidentiality and avoid unnecessary exposure of sensitive information.

7. Communication and Information Sharing

Foundation-related communication must be conducted in a secure and professional manner.

Sensitive information should be shared only with persons who need access and through appropriate channels.

Particular care must be taken when sending emails, sharing links, forwarding documents, using messaging platforms, or communicating about partners, beneficiaries, participants, or internal matters.

Information must not be disclosed informally or through insecure channels where this creates unnecessary risk.

8. Use of Personal Devices and Accounts

Where personal devices or accounts are used for Foundation work, the same standards of care, confidentiality, and security apply.

Foundation-related files, contacts, and communications should, where possible, be kept separate from purely personal use.

The Foundation may require that certain information or access be transferred, secured, or removed when an engagement ends.

9. Sensitive and High-Risk Information

Special care must be taken with sensitive information, including personal data, financial information, internal organisational matters, legal materials, safeguarding-related information, and any information relating to vulnerable persons, human rights defenders, LGBT+ persons, minority communities, or partners operating in hostile environments.

Access to such information must be strictly limited and handled on a need-to-know basis.

10. Cybersecurity Risks and Good Practice

All persons acting on behalf of the Foundation must exercise caution in relation to phishing, suspicious emails, fraudulent links, unknown attachments, account compromise, impersonation, malware, or other digital threats.

Suspicious activity or possible compromise must be reported immediately.

Users should avoid downloading unnecessary software, using unsecured networks for sensitive work, or bypassing reasonable security precautions.

11. Incidents and Reporting

Any actual or suspected digital security incident, including loss of device, account compromise, unauthorised access, accidental disclosure, suspicious activity, or data breach, must be reported immediately to the Executive Director or designated responsible person.

The Foundation shall take reasonable steps to contain, assess, and respond to security incidents in a timely and proportionate manner.

Where relevant, incidents must also be handled in accordance with the Data Protection Policy.

12. Responsibility and Oversight

All persons acting on behalf of the Foundation are responsible for protecting information and following this policy in practice.

The Executive Director is responsible for oversight of implementation, risk awareness, and ensuring that reasonable safeguards are in place.

The Board has oversight responsibility for ensuring that the Foundation takes digital and information security seriously as part of good governance.

13. Breach of Policy

Failure to comply with this policy may result in corrective or disciplinary action, depending on the seriousness of the breach.

Serious negligence, deliberate misuse, concealment of incidents, or unauthorised disclosure of sensitive information may be treated as a serious violation.

14. Related Policies

This policy should be read together with the Data Protection Policy (GDPR), Document Retention and Archiving Policy, Code of Conduct, Safeguarding Policy, Anti-Corruption and Fraud Prevention Policy, and any relevant legal or donor requirements.

15. Review of the Policy

This policy shall be reviewed periodically and updated as necessary to reflect organisational practice, digital risks, legal obligations, and good governance standards.