SAFEGUARDING AND SECURITY PROTOCOL

AFRICAN TECHNOLOGY POLICY STUDIES NETWORK (ATPS)

+254 020 2714092
info@atpsnet.org

AFRICAN TECHNOLOGY POLICY STUDIES NETWORK (ATPS)

8th Floor, Chancery Building, Valley Road
P. O. Box 10081-00100, Nairobi, Kenya
Email: executivedirector@atpsnet.org
Phone No: +254-202714092

SAFEGUARDING AND SECURITY PROTOCOL

The objective of this security protocol is to establish a robust framework that ensures the protection, confidentiality, integrity, and availability of sensitive information, physical assets, and personnel and beneficiaries of the African Technology Policy Studies Network (ATPS). By implementing this protocol, ATPS aims to mitigate risks, prevent unauthorized access, safeguard data, and respond effectively to security incidents affecting the institution, its staff, associates, network members, and project beneficiaries.

1. Governance and Risk Management:

a) Establish a security governance structure with clearly defined roles, responsibilities, and accountability for security-related matters.

b) Conduct regular risk assessments to identify vulnerabilities, threats, and risks to ATPS's information systems, physical facilities, and personnel.

c) Develop and maintain a risk management plan that outlines risk mitigation strategies, controls, and risk treatment processes.

d) Continuously monitor and evaluate the effectiveness of risk management activities.

2. Physical Security:

a) Implement physical security measures, including access control systems, surveillance cameras, and security personnel, to protect ATPS's premises and assets.

b) Establish visitor management protocols to ensure authorized access and monitor visitor activities.

c) Implement procedures for handling physical security incidents, including theft, unauthorized entry, or emergencies, and conduct regular drills and training exercises.

d) Maintain an inventory of physical assets and conduct periodic audits to ensure their security.

3. Information Security:

a) Develop and enforce an information security policy that covers the protection, handling, storage, transmission, and disposal of sensitive information.

b) Implement access controls, such as user authentication, authorization mechanisms, and role-based access controls, to ensure authorized access to systems and data.

c) Regularly update and patch software systems, employ firewalls, intrusion detection systems, and encryption technologies to protect against cyber threats.

d) Conduct periodic security awareness training for employees and stakeholders to promote a security-conscious culture and educate them about common security risks and best practices.

e) Establish incident response procedures to handle and report security incidents promptly, including data breaches, malware infections, or unauthorized access attempts.

f) Regularly back up critical data and establish robust disaster recovery and business continuity plans.

4. Network Security:

a) Implement secure network architecture, including segmented networks, network monitoring, and intrusion prevention systems.

b) Employ strong network access controls, such as virtual private networks (VPNs), to protect data transmitted over public networks.

c) Regularly assess and update network security configurations, including routers, switches, and firewalls.

d) Conduct periodic vulnerability assessments and penetration testing to identify and address network vulnerabilities.

5. Personnel Security:

a) Implement a comprehensive personnel security program, including background checks, confidentiality agreements, and security awareness training.

b) Define clear security roles and responsibilities for employees and ensure appropriate access controls based on job roles and responsibilities.

c) Establish processes for managing employee onboarding, offboarding, and role changes to ensure that access privileges are granted or revoked promptly.

d) Foster a culture of security awareness and accountability among employees through ongoing training and communication.

e) In case of insecurity incidences in the country of project implementation, the following needs to be considered and acted upon:

- Use local security experts: Local security experts will be familiar with the specific security threats in the country and will be able to provide guidance to the ATPS team through the National Chapter Coordinators on how to mitigate them.

- Use secure communication channels: All communication related to the project should be conducted using secure channels, such as encrypted email and chat applications where necessary.
- Be aware of the political climate: The political climate in the country can change rapidly, so it is important to be aware of the latest developments and to adjust the security protocol accordingly. ATPS National Chapter Coordinators will support in this.
- Have a contingency plan: In the event of a security incident, it is important to have a contingency plan in place. This plan will outline the steps that will be taken to respond to the incident and to minimize the damage. ATPS will commit all resources available to implement this.

6. Third-Party Security:

a) Perform due diligence on third-party vendors and partners to assess their security practices before engaging in any business relationship.

b) Establish and enforce contractual agreements that define security expectations and requirements for third parties handling ATPS's data or systems.

c) Regularly review and monitor the security practices of third-party vendors and conduct audits or assessments as needed.

7. Compliance and Legal Considerations:

a) Ensure compliance with relevant laws, regulations, and standards pertaining to data protection, privacy, and security in the jurisdictions ATPS operates in.

b) Establish mechanisms to monitor and adapt to changes in applicable laws and regulations.

c) Maintain appropriate documentation, consent forms, and privacy policies to demonstrate compliance with data protection regulations.

8. Incident Management and Response:

a) Develop an incident management plan that outlines procedures for detecting, reporting, and responding to security incidents promptly.

b) Establish an incident response team responsible for coordinating and executing incident response activities.

c) Regularly conduct security incident drills and tabletop exercises to test the effectiveness of incident response plans and identify areas for improvement.

d) Maintain incident logs, conduct post-incident reviews, and implement lessons learned to enhance future incident response efforts.

9. Continuous Improvement:

a) Establish a process for ongoing monitoring, assessment, and improvement of ATPS's security posture.

b) Regularly review and update security policies, procedures, and controls to align with emerging threats, technological advancements, and regulatory requirements.

c) Encourage feedback from employees, stakeholders, and security professionals to identify areas for enhancement and address evolving security challenges.

10. Insurance Coverage:

a) Assess the insurance needs of ATPS and obtain appropriate insurance coverage to mitigate risks on ATPS personnel, its associates' finances associated with security incidents, including property damage, data breaches, liability claims, and business interruption.

b) Consult with insurance professionals to identify the specific types of insurance policies required, such as property insurance, cyber liability insurance, professional liability insurance, and business interruption insurance.

c) Review and update insurance policies periodically to ensure they align with ATPS's evolving security risks and operational changes.

d) Maintain proper documentation of insurance policies, coverage limits, deductibles, and contact information for insurers.

e) Develop procedures for promptly reporting security incidents to insurers and filing insurance claims when necessary.

f) Conduct periodic reviews and assessments of insurance coverage to ensure it adequately addresses ATPS's security risks and potential liabilities.

11. Risk Transfer and Indemnification:

a) Establish contractual agreements with third-party vendors, partners, and service providers that include provisions for risk transfer and indemnification.

b) Include clauses that require third parties to maintain adequate insurance coverage and provide proof of coverage.

c) Review and negotiate indemnification clauses to allocate risks appropriately and protect ATPS from potential financial losses resulting from third-party actions or failures.

d) Consult with legal advisors to ensure the language in contracts effectively transfers risk and provides necessary protections for ATPS.

12. Claims Handling and Recovery:

a) Develop a claims handling process to streamline the reporting and resolution of insurance claims.

b) Designate a responsible individual or team within ATPS to oversee the claims handling process and liaise with insurers.

c) Maintain detailed records of security incidents and related damages or losses to support insurance claims.

d) Collaborate with insurers during the claims process, providing all necessary documentation, evidence, and information requested.

e) Monitor the progress of insurance claims and follow up as needed to ensure timely and fair resolution.

f) Develop a contingency plan to address potential gaps in insurance coverage, such as self-insurance or alternative risk management strategies, to mitigate risks that cannot be fully transferred through insurance.

Note: This Security Protocol provides a foundation for ATPS to develop detailed security policies, guidelines, and practices tailored to its specific needs and operating environment. Regular assessments, employee training, and continuous improvement efforts are essential to ensure the effectiveness of security measures and adapt to evolving security risks.

Contact Us

+254 020 2714092

info@atpsnet.org

https://atpsnet.org/

8th Floor, The Chancery, Valley Rd, Nairobi, Kenya