EPF's Information Security Policies

Last
Revised
Date:
February
2022

Yerevan, Armenia

Preface

Eurasia Partnership Foundation – Armenia (EPF) is prioritizing safe and secure communication in conducting its operations. EPF's commitment in maintaining the highest standards of information security — both inside and outside the organization — is thoroughly developed and periodically revised in its official documents. Besides, it is an ethical standard as well practiced in all levels of communications of the staff, the partners, beneficiaries, donors and beyond. The risks and threats brought by technological and information advancement provides clearer understanding of the necessity to constantly review the policies on Information Technologies' (IT) security, data protection, and mindful usage. The following compendium comprises EPF's official documentation pertaining to its IT Security Policy, EPF Cybersecurity Risk Assessment, required steps to address the risk (titled as EPF Cybersecurity Action Plan), further recommendations from "Helping EPF Mitigate Cybersecurity Risks" report, and EPF IT Security Plan.

1. Information Security Policy

Purpose

The purpose of the information security policies and procedures of EPF are to insure the following goals:

- To provide high quality IT services;
- To ensure the integrity and validity of data;
- To enable the effective and efficient recovery of data after disruption in IT services; and
- To protect of all EPF's IT assets including data, software, and hardware.

The above services, data, and assets include computer systems, data networks, user workstations, and telephones.

IT Manager Responsibilities

The IT Manager shall provide leadership and direction for EPF's network and systems security. The IT Manager shall develop and implement a network architecture that places an emphasis on security. A single compromised workstation can be used to attack other systems both within and outside EPF.

The IT Manager is responsible for establishing, communicating, and enforcing unit level practices and procedures that promote security. The following areas should be covered:

- Physical security.
- Protection of information, which includes periodic backup and offsite rotation of mission critical systems, applications, emails, websites and data files.
- Prevention of unauthorized access.
- Detection of security breaches.
- Procedures for reporting security breaches to management or appropriate authority.
- Change all passwords every six months
- Regularly upload the backups to the Cloud
- Regularly store the version of cloud services on local server
- Regular backup of corporate emails.

The IT Manager will work with other IT managers in EF Network to find and correct problems. A user's access privileges may be temporarily suspended if the IT Manager believes it is necessary or appropriate to maintain the integrity of the computer system or network.

Users' Responsibilities

EPF staff must comply with the following policies:

- Staff must have a valid authorized account to use computer resources, when required and may use only those computer resources that are specifically authorized for their use;
- Staff may only use computer account in accordance with authorized purposes and may not use an unauthorized account for any purpose;
- Staff shall not circumvent system protection facilities.
- Staff may not use computer resources for private purposes, including, but not limited to, the use of computer resources for profit making or illegal purposes;
- Staff must get approval from senior management and inform the IT manager when taking any IT equipment outside the office. A log is available at the reception to sign in and out any traveling equipment. In the case of loss or damage of equipment during travel, the President/CEO and IT Manager determine the level of responsibility of the staff.
- Staff should not use the same password for different platforms.
- The passwords should be changed at least every six months, even if the system doesn't suggest it.
- Be sure to enable 2 step verification for websites.

Hardware Policy

The effect of electrical power outages and fluctuations shall be protected against by the installation of uninterrupted power supplies (UPS) and surge protection devices.

Requests for additional hardware not included in the standard basic desktop configuration shouldbe approved by President/CEO or the Chair of the Board of Trustees (if the hardware is requested by the President/CEO).

Printers, Scanners, and Copiers

The IT manager is responsible for maintaining EPF's printers, scanners, and copiers; however, all staff is responsible for proper and safe use for printers and scanners.

Software Policy

All materials associated with any computer system, including software and printed materials thatare not in the public domain, must be treated in accordance with any applicable copyright agreements, restrictions and usage agreements.

The IT manager installs a basic suite of software applications during the initial computer installation. The staff members should have a standard "user's permission without admin rights" window on their local computers/devices.

Requests for additional applications not included in the basic suite of software applications must be approved by the President/CEO.

Any software that has the potential to interact with networking facilities must not be installed or

run on any computer connected to EPF's Local or Wide Area Networks without the approval ofthe President/CEO:

Any other software will be installed on user's devices only after approval by the management and IT Manager's testing.

Network Storage

It is strongly recommended that network drives are utilized to save files and data. The IT manager does not back up personal files saved on the local hard drive of individual computers.

The Network Drive has been created in order to protect EPF data from loss and to increase data availability. The contents of the Network Drive are backed up on a daily basis and can be promptly restored anytime. Every department is urged to keep its important business related dataon the Server.

Data Security Policy

An appropriate, regular, back-up schedule shall be implemented by the IT manager to protect all server-based data and software deemed critical.

No EPF staff member may use a computer system or any account, or otherwise attempt to access any file or device to access, modify, or disclose information that he or she is not authorized to use or possess.

Highly sensitive data must be password protected and encrypted.

Internet Security Policy

The Internet should be treated as a potentially hostile environment. For many systems, access to the Internet will be via a Firewall. The local area network should be under protection, under intrusion prevention system and content detection.

All traffic passing through an account may be logged and may be audited. EPF's network system will be monitored and checked. A black list for restricted sites will be updated regularly.

Virus Protection Policy

Viruses can enter EF network in a variety of ways, including through email, CD or removable data storage device, downloading from the Internet, or instant messaging attachments

It is the responsibility of everyone who uses EPF's computer network to take reasonable measures to protect that network from virus infections. This includes the following list of recommended procedures:

- Staff should never open an e-mail attachment if you do not recognize the sender;
- If a staff member receives a suspicious file or e-mail attachment, do not open it. Notify the

IT manager; s/he will explain how to handle the file.

If a file is an infected spreadsheet or document that is of critical importance to EPF, the IT manager will attempt to scan and clean the file. The IT manager, however, s/he makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on EPF computers.

Network Connections

All equipment to be connected to EPF's data and voice network should be approved by IT manager.

2. List of EPF IT Policy Documents

Annex 2.1 EPF Cyber-Security Risk Assessment Document

Executive Summary

The Eurasian Partnership Foundation (EPF) leverages community activism and philanthropy to build peaceful cooperation among people in the South Caucasus region. As a part of the USAID efforts to assess and improve the security posture of their beneficiaries, USAID engaged Stratigos Security to perform a Cybersecurity Risk Assessment and to develop Cybersecurity Action Plans. the project evaluated technical systems for resilience against known adversary attack patterns, performed a risk assessment according to the SAFETAG framework, and mapped organizational cybersecurity maturity against the Center for Internet Security top 20 Controls.

Summary of Cybersecurity Risks

Stratigos identified organizational risks based on elicitation sessions, interviews, and technical analysis. Key stakeholders voiced several concerns during an initial risk discussion, which were validated during subsequent steps. In addition, workflow analysis with individual staff members and technical testing of the internal and external network revealed other risks which are accounted for below:

- Hacking of the websites
- Hacking of corporate emails
- Unauthorized access to the organization's internal database
- Personal data about beneficiaries
- Physical security of the office

Summary of Risk Mitigation Actions

EPF has a fairly mature cybersecurity program for its size and industry, as measured by standard security benchmarks, such as the Center for Internet Security top 20. While their size and resources limit their ability to protect against high-capability cybersecurity threat actors, it's clear they have invested in their own capabilities. EPF's cybersecurity goal is to make attacks more apparent, delay their effect, and respond quickly and effectively. to improve in several key areas, EPF should take the following actions:

- Use fully updated, supported website software
- Implement full disk encryption
- Implement Virtual Private Network (VPN) for office connectivity

Some Action Items can be implemented in parallel and improve security while the longer-term projects are underway.

- Implement Password Management Software
- Implement Multi-Factor Authentication
- Multi-User Management for Social Media Accounts

Finally, Pink will need support from an It support specialist to implement and maintain all these actions. Full detail of these risk mitigation Action Items can be found in the EPÏ - Cybersecurity Action Plan document.

Assessment Methodology

Data Collection and Project Initiation

During this phase, we formally kick off the project, collect relevant documentation, and schedule project activities at a finer level. this ensures information and individuals are available to reduce undue delay, but with enough flexibility to accommodate inevitable changes. We will work with you to determine most relevant documents to review and personnel to meet. A kickoff meeting ensures all key stakeholders are introduced, either in person or virtually, establishes communications trees, and ensures a clear understanding of the project.

SAFETAG Framework

The Security Auditing Framework and Evaluation template for Advocacy Groups (SAFETAG) Framework is developed by and for non-governmental organizations, civil society organizations, and non-profit cybersecurity groups. the process begins with an organizational risk assessment, which gives insight into key cybersecurity threats and concerns the beneficiary faces. Next, individual interviews provide a cross section of the people, process, and technology cybersecurity. In addition, technical scanning across the organization's entire network and set of systems provides information on software and configuration vulnerabilities.

CIS CSAT Evaluation

Our consultants led a facilitated evaluating leveraging the Center for Internet Security (CIS) Controls Self-Assessment tool (CSAT) to gauge organizational maturity in a consistent, standardized way. this methodology takes a top-down approach to understanding organizational cybersecurity controls based on the CIS top 20. Survey responses are mapped against industry averages to visually show how the beneficiary's cybersecurity maturity compares against a sample of other organizations.

Internal/External Network Vulnerability Assessment

An external network penetration test consists of several iterative phases. Stratigos uses the Penetration testing Execution Standard (PTES)[1], an industry-recognized methodology, as the basis for our testing. Depending on the types of adversaries and attacks simulated, the methodology may vary from project to project.

[1] Penetration testing Execution Standard http://pentest-standard.org

- **Intelligence Gathering and Scope Verification** – through open source intelligence gathering (OSINT) and other methods, the tester attempts to passively and actively gather information about the target environment. During this phase, the scope is compared against the intelligence gathered to verify that there are no gaps or misalignments.
- **Threat Modeling** – During this phase, Stratigos tailors adversarial attack patterns to your business and technical environment. this step ensures work efficiently mimics real-world threats, and that results align to business objectives.
- **Vulnerability Assessment and Analysis** – Stratigos attempts to determine vulnerabilities through automated and manual processes, by interacting with services on open ports. this includes testing known vulnerabilities, password guessing, web intrusion attempts, and other techniques.
- **Evidence Collection** – Stratigos identifies target assets and captures evidence sufficient to demonstrate findings to management.

Stratigos uses industry-leading and custom built tools to probe the network for potential vulnerabilities. the findings are analyzed to identify potential risk vectors, such as:

- Potential rogue devices, including wireless clients and access points
- Common, default credentials
- Known but unmitigated software flaws
- Common configuration weaknesses
- Deviations from industry or organizational standards (such as CIS 20 Controls and OWASP top 10 Vulnerabilities)

Technical artifacts were provided to the technical points of contact for the organization.

SAFETAG Cybersecurity Risk Assessment

The SAFETAG methodology includes conducting a cybersecurity risk assessment that captures both systemic issues and individual vulnerabilities. the initial organizational risk assessment session was attended by several key stakeholders, including the part time It support staffer. this was followed by interviews and facilitated technical reviews with 5 employees, 5 computers, and 5 phones. In addition, technical reviews were conducted on the internal network, wifi network, website, constituent relationship management system, primary Facebook pages, and corporate email.

Hacking of the websites

Stratigos found serious problems with its 3 websites: epfarmenia.am, kronadaran.am, and hkdepo.am. Epfarmenia.am is an outdated Drupal installation on an Ubuntu 18.04 server, with an outdated version of php 7.2. the website is protected by Cloudflare's Galileo service, which has special rules for protecting Drupal, which provides a stopgap until the site can be updated to mitigate or eliminate the vulnerabilities. Kronadaran.am is running an unsupported version of Wordpress with several vulnerable plugins that could lead to defacement or attack against site visitors. Hkdepo.am is a custom written site using the PHP/Laravel framework. It is also
protected by Cloudflare and outside scan didn't reveal any vulnerabilities.

Recommendation: Maintain internet-facing websites with due care by ensuring they are running supported versions and applying software security updates promptly. Develop and implement a management program to ensure that platform migrations happen with ample time to avoid going out of support.

Responsibility: EPF's management, IT manager, webmaster, external web developer

Hacking of corporate emails

the organization uses GSuite, which is centrally managed from the Admin Console. there is no corporate email policy, some mailboxes are accessed by more than one employee, Multi-Factor Authentication (MFA) is optional and not everyone uses it. the organization doesn't have a password management policy or system either, with some employees admitting that they use the same password for several accounts.

Recommendation: Enable MFA for all GSuite accounts, develop a corporate email policy, carry out password training for the employees and consider using password management software like 1Password or LastPass to centrally manage and enforce password policies.

Responsibility: EPF's IT manager, external digital security trainer

Unauthorized access to the organization's internal database

The organization is partly protected. the internal database is a custom written php/MySQL web application, which resides in the internal network and is usually closed for the outside world. However, due to COVID-19 it has been occasionally opened for the outside world, so that the remote workers can access it. the code is custom written and not updated, the underlying architecture is old and has a range of vulnerabilities, including some that may lead to complete system compromise.

Recommendation: In the short term the organization should consider configuring secure VPN access to the office and stop the practice of opening up the internal database to the outside world, but instead have the work from home employees connect to the office network via VPN. In the long term, the organization should find resources to update the internal database system or invest in licensed and up to date CRM/Database system, which can serve those needs.

Responsibility: It manager, organization's management

Personal data about beneficiaries

The organization uses a special accounting software. Since the license is very expensive, several people access it using the same password. the remaining programmatic documents: lists of participants, personal data of people involved in project, budgets and financial data are often shared via corporate email, some employees sometimes send files to their personal emails to be able to work from home. Some programmatic data is also shared via Facebook messenger.

Recommendation: Establish a data sharing policy and decide on a more suitable cloud storage

solution, which would allow to secure the data and establish proper file sharing and access controls, invest in more licenses of the accounting software to accommodate the needs.

Responsibility: Chief accountant, It manager

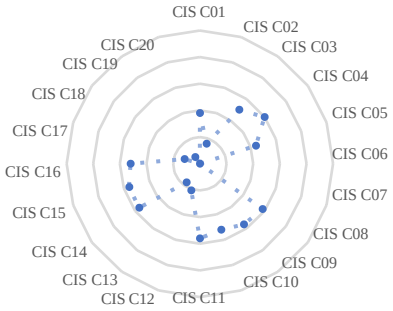
Physical security of the office

The organization is not protected. the computers are not encrypted, there are no security cameras in and around the office, the office doesn't have metal bars on the windows, and the server room is unprotected against physical entry.

Recommendation: Encrypt all office computers and servers, and invest in security cameras. Consider investing in physical security of the building, possibly with the help of physical security consultant.

Responsibility: It manager, organization's management

CIS Controls Self Assessment tool Results



The Center for Internet Security (CIS) publishes a list of 20 security controls they consider to be foundational to an effective cybersecurity program. USAID beneficiaries undertaking the Digital APEX program are assessed against this list of controls using the CIS Controls Self Assessment tool (CSAT) so they can be benchmarked against future progress, other beneficiaries, and industry averages. the tool measures the number of maturity markers for each of these controls and presents the information as a completeness percentage (0-100% of markers in place).

EPF scored very highly on the CIS CSAT for their size and level of resourcing. Notable outliers include controls around monitoring and auditing, and email and browser protections, as those are typically higher in organizations of their maturity. During the engagement Stratigos provided instructions and guidance to address these deficiencies and those recommendations appear in the Action Plans mentioned in the executive summary.

Control	Score
1. Inventory and Control of Hardware Assets	38%
2. Inventory and Control of Software Assets	16%
3. Continuous Vulnerability Management	50
4. Controlled Use of Administrative Privileges	60%
5. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	44%
6. Maintenance, Monitoring, and Analysis of Audit Logs	0%
7. Email and Web Browser Protections	0%
8. Malware Defenses	58%
9. Limitation and Control of Network Ports, Protocols, and Services	56%
10. Data Recovery Capabilities	52
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	56%
12. Boundary Defense	21%
13. Data Protection	17%
14. Controlled Access Based on the Need to Know	56
15. Wireless Access Control	56%
16. Account Monitoring and Control	52%
17. Implement a Security Awareness and training Program	12%
18. Application Software Security*	--*
19. Incident Response and Management	6%
20. Penetration tests and Red team Exercises*	--*
* Control category not assessed in the version of the CSAT used	

Conclusion

It is clear that EPF values cybersecurity and its investment have paid benefits. their personnel are knowledgeable and diligent, their technology is generally well maintained, and they have an environment of security consciousness. However some risky practices remain that the It staff are working to resolve. With attention to these few areas, EPF can significantly raise their resilience and recoverability against accidents and adversaries.

Annex 2.2 EPF Cyber-Security Action Plan

Executive Summary

The Eurasian Partnership Foundation (EPF) leverages community activism and philanthropy to build peaceful cooperation among people in the South Caucasus region. As a part of the USAID efforts to assess and improve the security posture of their beneficiaries, USAID engaged Stratigos Security to perform a Cybersecurity Risk Assessment and to develop Cybersecurity Action Plans. The project evaluated technical systems for resilience against known adversary attack patterns, performed a risk assessment according to the SAFETAG framework, and mapped organizational cybersecurity maturity against the Center for Internet Security Top 20 Controls.

Summary of Findings and Recommendations

EPF operates like a small business, though it faces highly capable motivated adversaries. EPF has a fairly mature cybersecurity progr for its size and industry, as measured by standard security benchmarks, such as the Center for Internet Security top 20. Whil their size and resources limit their ability to protect against high-capability cybersecurity threat actors, it's clear they have invested their own capabilities.

EPF's cybersecurity goal is to make attacks more apparent, delay their effect, and respond quickly and effectively. to improve in several key areas, EPF should take the following actions:

- Use fully updated, supported software
- Implement full disk encryption
- Trusted encrypted communications platforms
- Implement Virtual Private Network (VPN) for office connectivity
- Implement Password Management Software
- Implement Multi-Factor Authentication

Action Plan

Each of the pages below contains a single Action Item that will help EPF build capacity for a sustainable security program. Most of the Action Items can be implemented on a modest budget in the coming weeks or months without significant disruption to workflow. Some of theAction Items represent roadmap projects to be implemented when certain conditions and thresholds are met, as articulated in the plan.

The information provided represents an independent third-party recommendation intended to assist in justifying additional funding from donors. Where specific expertise or resources are required to implement the items, Stratigos has estimated initial implementation as well as ongoing needs.

EPF has invested in It and cybersecurity capabilities so the list of action items is short. However, there are some key initiatives that, if undertaken, can significantly raise their securityposture and improve resilience against accidents and adversaries.

The accompanying **EPF – Cybersecurity Risk Assessment** document contains detail on risks identified and the table below maps these to Action Item(s) that help in mitigating these risks.
In addition, there are further recommendations specific to those risks which may partially address these issues though don't rise to the level of an Action Item. In addition, there are some Action Items which are considered effective practice and are low effort, which do not directly relate to the organization's largest risks.

Cybersecurity Risk Assessment	**Action Item(s)**
Hacking of the websites	Use fully updated, supported software
Hacking of corporate emails	Implement Password Management Software Implement Multi-Factor Authentication
Unauthorized access to the organization's internal database	Implement VPNs for office connectivity Implement Password Management Software Implement Multi-Factor Authentication
Personal data about beneficiaries	Use fully updated, supported software Implement Password Management Software Implement Multi-Factor Authentication trusted encrypted communications platforms
Physical security of the office	Implement full disk encryption

Use Fully Supported, Updated Website Software

Description Maintain internet-facing websites with due care by ensuring they are running supported versions and applying software security updates promptly. Develop and implement a management program to ensure platform migrations happen with ample time to avoid going out of support.	**Justification** Websites directly expose organizational infrastructure to adversaries over the Internet. Even sites that do not contain sensitive information or provide a direct pathway to internal systems can pose risks to reputation or site visitors if compromised.
When to initiate Implement as quickly as reasonably possible, ideally by deploying a new server in parallel for testing, then migrate to the fully updated instance. If new sites or servers are in development, ensure that they are running the latest versions of the operating system, web platform, and any site components.	**Success criteria** A recurring authenticated vulnerability or configuration scan on the organization's website can validate the action is consistently taken. In addition, uncredentialled scanning can give some insight into vulnerabilities most likely to be exploited by adversaries

Resourcing		

Estimated Cost Capital: None unless new licenses are required Operating: Minimal	**Estimated timeline** 1-2 Weeks	**Required Skillset** Basic It administration and web skillset

Implement Full Disk Encryption

Description Full Disk Encryption (FDE) is a technology which protects information and data stored on a hard drive by converting it into unreadable code that cannot be deciphered easily. Implement FDE on computers and mobile devices.	**Justification** Adversaries with physical access to a device can retrieve sensitive information that puts the organization, its employees, and its beneficiaries at risk. For instance, passwords for bank accounts or online services; personal data about clients or employees; or other protected information.
When to initiate Organizations of all size and maturity should implement this action as soon as possible.	**Success criteria** Tools like Windows BitLocker are provided by Operating System vendors free of charge. BitLocker can be trivially verified on the device or through automated configuration scanning.

Resourcing		
Estimated Cost Capital: None Operating: Minimal	**Estimated timeline** 1 week or less	**Required Skillset** Basic It administration skillset

Trusted Encrypted Communications Platforms

Description Protecting communications is of utmost importance when working with vulnerable populations. train employees and constituents to use highly secure platforms, such as Signal, when sending sensitive information.	**Justification** When dealing with high capability adversaries, carrying out potentially sensitive work, all due care should be taken to ensure communications are not intercepted. While telegram is an excellent tool for reaching the public, it is not considered to be one of the more secure communications platforms, even considering the “Secret Chat” feature.

When to initiate Organizations of all size and maturity should implement this action as soon as possible.	**Success criteria** Select platforms that enforce strong end-to- end encrypted communication, with the ability to verify identity and authenticity, and that have had extensive, publicly available security auditing. Stratigos recommends Signal, which meets these criteria.

Resourcing		
Estimated Cost Capital: None Operating: Low	**Estimated timeline** **1-2 weeks**	**Required Skillset** Basic It administration skillset

Implement a Virtual Private Network (VPN) for Office Connectivity

Description Virtual Private Networks (VPNs) can help avoid censorship and evade eavesdropping. VPNs can also allow organizations to restrict access to sensitive or highly critical resources on internal networks. Many network border devices provide VPN capabilities to allow secure access to internalnetwork resources.	**Justification** Sensitive resources and databases on the internal network exposed to the Internet posean unacceptably high risk. VPNs significantlymitigate these risks, especially when combined with multifactor authentication.
When to initiate Organizations that need to provide remote access to internal network resources should implement this action as soon as possible, provided they have basic It administration skills to implement and maintain it.	**Success criteria** Stratigos has developed a VPN evaluation framework (Appendix A) to help decisionmakers select VPN options.

Resourcing		
Estimated Cost Capital: None Operating: Low	**Estimated timeline** **1-2 weeks**	**Required Skillset** Basic It administration skillset

Implement Password Management Software

Description Password management applications automatically generate, store, and use strong, unique credentials for each internal or cloud- based system. Provide password management software for all employees and enforce its usage.	**Justification** Credential attacks are the largest security threat most organizations face, in large part because authentication mechanisms are designed to work well for computers and not people. Password management software makes it easy and inexpensive to generate, maintain, and use high security credentials for internal and cloud-based systems. Their low cost and ease of use may improve employee productivity and efficiency. Central management further improves management control over It assets.
When to initiate Organizations of all size and maturity should implement this action as soon as possible. Organizations with a basic It skillset can take advantage of central management capabilities.	**Success criteria** Select password management software that provides local language support, centralized management, and multi-platform integration. Many password managers flag credentials that have been recently breached and automate updating passwords.

Resourcing		
Estimated Cost Capital: Minimal, especially for non- profits Operating: Minimal, especially for non-profits	**Estimated timeline** 1-3 weeks	**Required Skillset** No special skillset

Implement Multi-Factor Authentication

Description Multi-Factor Authentication (MFA) greatly increases account protection, especially for cloud-based services. By augmenting password authentication with physical tokens or temporal codes, adversaries that acquire a password are still prevented from gaining access to a system. Implement MFA on compatible systems, including email, website, and cloud based data storage.	**Justification** Credential attacks are the largest security threat most organizations face. Adding a second factor of authentication reduces this risk by at least an order of magnitude. Multi- Factor Authentication (MFA) is relatively inexpensive, low friction, and low implementation cost for most systems.
When to initiate Organizations of all size and maturity should implement this action as soon as possible on Internet-facing services that make the capability available.	**Success criteria** Select technologies that are easy to use and low or no cost, and that provide app-based or token-based authentication. High capability adversaries can easily intercept or tamper with SMS-based authentication factors, so avoid those.

Resourcing		
Estimated Cost Capital: Low to none Operating: Minimal	**Estimated timeline** 2-3 weeks	**Required Skillset** Basic It administration skillset to implement, no special skillset to use

Conclusion

It's clear that EPFs executives and staff are concerned about cybersecurity and have used a share of their limited resources to build up infrastructure, employ It personnel and train their staff in cybersecurity practices. It is also clear that the organization would benefit from moreinvestment in their infrastructure and up to date, licensed software improve their security posture to counter the high capability adversaries they face.

Appendix A: VPN Selection Framework

The virtual private network (VPN) selection framework was developed by Stratigos Security to facilitate decision-making by management when evaluating alternatives, whether self-hosted or commercial services.

Management

- **Implementation -** Difficulty and cost in implementing the VPN server or service, given the organization's financial and technical capabilities.
- **Operating expense -** Ongoing cost (per month, per seat) for the VPN, including employee training (if necessary).
- **Provisioning -** Ease of adding new accounts onto the platform.
- **Scalability -** How many total or concurrent accounts the server can support.

Ease of Use

- **Acceptability -** Ease of use for employees and others utilizing the VPN day-to-day.
- **Client availability -** Whether the VPN has clients to support all platforms that the organization uses.
- **Language support -** Whether VPN clients support all the languages in use within the organization.

Supply Chain

- **Proximity -** Relative location of the VPN server or service to resources and individuals using the VPN, which can affect speed and integrity of the connection.
- **Legal policies -** National or local policies on data interception, individual surveillance, or others, which may compel the service provider to degrade the integrity or confidentiality of the VPN connection.
- **Code and component transparency -** How transparent is the software or service provider about third-party and open source code, and partnerships (for instance, their cloud and VPN provider).
- **Logging -** Whether the software or service keeps connection logs or other information which could uniquely identify individual or organizational traffic.

Security assurance

- **Third-party attestation -** Whether the software or service provider have regular third- party security assessments with attestation, from reputable security firms.
- **Protocol security -** Security of the encryption protocol selection and implementation.
- **Network detection avoidance -** Difficulty for local network providers to detect (and potentially block) VPN traffic.
- **Disconnect security -** Whether the VPN prevents data leakage before it is connected or when the connection terminates.
- **Tenant isolation -** the degree to which accidents and adversaries affecting one host, region, or IP address will affect all VPN tunnels.

Annex 2.3 Recommendations from "Helping EPF Mitigate Cybersecurity Risks" Report

Recommendations from "Helping EPF Mitigate Cybersecurity Risks" Report **Presented to Eurasia Partnership Foundation** **By: Beau Woods Founder/CEO Stratigos Security** **Published September 10, 2021** **EPF Responses as of January 21, 2022**	
Findings and Recommendations	EPF's Response
1. Hacking of the websites **Description:** Stratigos did not find.am, kronadaran.am, and hkdepo.am. Epfarmenia. Serious problems with EPF's 3 websites: epfarmenia am is an outdated Drupal installation on an Ubuntu 18.04 server, with an outdated version of php 7.2. The website is protected by Cloudflare's Galileo service, which has special rules for protecting Drupal, which provides a stopgap until the site can be updated to mitigate or eliminate the vulnerabilities. Kronadaran.am is running an unsupported version of Wordpress with several vulnerable plugins that could lead to defacement or attack against site visitors. Hkdepo.am is a custom written site using the PHP/Laravel framework. It is also protected by Cloudflare and outside scan didn't reveal any vulnerabilities. **Recommendation:** Maintain internet-facing websites with due care by ensuring they are running supported versions and applying software security updates promptly. Develop and implement a	**Auditee comments:** The new website for Kronadaran.am is ready and launched. epfarmenia.am, hkdepo.am websites were build 5-7 years ago, but the websites are protected with firewalls, which will serve till the new websites are launched.

management program to ensure that platform migrations happen with ample time to avoid going out of support. **Responsibility:** EPF's management, IT manager, webmaster, external web developer	
2. Hacking of corporate emails **Description:** The organization uses GSuite, which is centrally managed from the Admin Console. There is no corporate email policy, some mailboxes are accessed by more than one employee, Multi-Factor Authentication (MFA) is optional and not everyone uses it. The organization doesn't have a password management policy or system either, with some employees admitting that they use the same password for several accounts. **Recommendation:** Enable MFA for all GSuite accounts, develop a corporate email policy, carry out password training for the employees and consider using password management software like 1Password or LastPass to centrally manage and enforce password policies. **Responsibility:** EPF's IT manager, external digital security trainer	**Auditee comments:** All EPF corporate emails are secured with 2-factor-authentification system, since November 1, 2021. From now on the system enforces corporate email holders to activate 2-factor-authenitification and change their passwords once six months. If a corporate email user doesn't change or activate 2-fatcor-authentification in the indicated period, the system automatically restricts the above mentioned accounts. The organization doesn't have a written password management policy yet, but it will be finalized and written till 15 February 2022.
3. Unauthorized access to the organization's internal database **Description:** The organization is partly protected. The internal database is a custom written php/MySQL web application, which resides in the internal network and is	**Auditee comments:** This issue is already solved, since the database is only for the users who are connected to EPF's local server. Database access is granted only to those users who have EPF corporate emails. EPF corporate emails since 1 November, 2021, are secured with 2-factor-authentification system. Anyway, depending on the financial resources, further actions will be taken for updating the database and taking more security actions.

usually closed for the outside world. However, due to COVID-19 it has been occasionally opened for the outside world, so that the remote workers can access it. The code is custom written and not updated, the underlying architecture is old and has a range of vulnerabilities, including some that may lead to complete system compromise. **Recommendation:** In the short term the organization should consider configuring secure VPN access to the office and stop the practice of opening up the internal database to the outside world, but instead have the work from home employees connect to the office network via VPN. In the long term, the organization should find resources to update the internal database system or invest in licensed and up to date CRM/Database system, which can serve those needs. **Responsibility:** IT manager, organization's management	
4. Personal data about beneficiaries **Description of the finding:** The organization uses a special accounting software. Since the license is very expensive, several people access it using the same password. The remaining programmatic documents: lists of participants, personal data of people involved in project, budgets and financial data are often shared via corporate email, some employees sometimes send files to their personal emails to be able to work from home. Some programmatic data is also shared via Facebook messenger.	**Auditee comments**: a) EPF has a special finance management software. The access to this software is granted to five user accounts. Assigned users are EPF finance team members: chief financial officer, finance manager, grants manager, EPF HR manager and one of the EPF program managers. EPF other program managers use the same password as the license for gaining additional user accounts is too expensive. EPF uses this finance management software for many years. It is a single source system. Approximately two years ago when the software developers team was changing the system, EPF was thinking about ordering such a local system, but it turned out to be more expensive. Currently EPF pays $530 monthly fee for finance management software. EPF development manager and program teams involved in fundraising will try to find additional funds for having more user accounts in the future. In accordance to EPF P&P the sensitive data extracted from finance managemnt software is stored only

Recommendation: Establish a data sharing policy and decide on a more suitable cloud storage solution, which would allow to secure the data and establish proper file sharing and access controls, invest in more licenses of the accounting software to accommodate the needs. **Responsibility:** Chief accountant, IT manager	on local server. The data is encrypted and backed up on a Cloud server. b) EPF staff members currently use only corporate emails. All the information (sensitive and not only) is shared via corporate emails. All EPF corporate email accounts are already secured with 2-factor-authentication system. A reminder to corporate email holders is sent once six months and the system enforces to change the passwords and to activate 2-factor-authentification. The corporate emails of those users who have not activated the 2-factor-authentication system are automatically enabled/restricted until they activate it. Use of personal emails for sharing work related data is prohibited by the EPF P&P. EPF employees can access their corporate emails from everywhere, using their corporate computers and other secure devices (EPF corporate emails are secured with 2-factor-authentification and computers are user password protected). EPF employees in some urgent cases (COVID19, war, and other emergency cases) can use EPF Synas storage system from distance, using a special folder created in Synas Transfer section protected with password, which has a 3-7 day expiration date upon request to IT manager. The sensitive information can be stored in this folder and the password is sent only to EPF staff member responsible for using this data. c) According to EPF P&P employees are prohibited to use FB messenger for sharing sensitive data. The FB messenger EPF group exists only for fast communication related to personal security or important external information, publications etc. This group has been created as a response to the 2020 crises – the pandemic and the war, in order to have an additional way of communication for the cases of emergencies. Only public information is shared via EPF FB messenger group. **Auditee response to recommendation:** EPF has a special file storing system, which is placed on its local server. EPF file server is called Synas. It consists of 2 sections: EPF NetDrive – all programmatic files (announcements, meeting notes, reports, publications, etc.) are stored in this folder and EPF Photo Station – all EPF photos from events/meetings/etc. go to this folder. EPF has a special folder system and a proprietary internal database. EPF regulates all its file storing systems in accordance to 'Institutional memory' procedures and guidelines. EPF also has a Contacts Database. The database is used for the

	management of EPF business contacts with relevant information and keywords, EPF programs database for putting basic information about the projects and storing the documents including the project proposals, budgets, interim and final reports. It also has a donors information (database) directly linked to programs database. EPF currently has 3 written documents (EPF Rules and Manual for contacts database, November 2014, EPF Communication Channels Guidelines, December 2017, EPF Contacts Database Guide on the mailing lists, June 2019) regulating data sharing procedures, till 15 February 2022 a compiled document on data sharing and storing management will be created. **Access controls** – EPF Financial software/ HOPE system has five user accounts. The access is granted by a system developer team under request of EPF finance team. The user accounts are created only with EPF corporate emails. EPF corporate emails are protected with 2-factor-authentification system. – EPF on-line banking access is granted only to limited members of Finance team, EPF chief executive officer and associate director. There are 'A' and 'B' categories of signatures. The employees holding an 'A' signature can only create payments and proceed with the payment only after the approval of the 'B' signature holders. 'B' signature holder approves the payment and gives consent to making financial transactions. – EPF Database can be accessed with individual username and password. The user account is created by Database admin. – EPF Photo Station access is granted to EPF program team with view-only option, program team members are not permitted to delete or edit files located in Photo station. EPF staff members can access EPF photo station only when they are connected to – EPF Net Drive can be accessed by EPF staff members only via corporate computers and in case of being connected to the local server. EPF Net Drive folders containing sensitive data are protected with user passwords granted by EPF IT manager.
5. Physical security of the office **Description of the finding:** The organization is not protected. The computers are not encrypted, there	**Auditee comments:** According to the standards, security cameras should be installed. Security cameras are installed around the building where the office of EPF is located including the parking space within the building. Additionally, the Embassy of United Arab Emirates is next to the building. The security serviceman of

are no security cameras in and around the office, the office doesn't have metal bars on the windows, and the server room is unprotected against physical entry. **Recommendation:** Encrypt all office computers and servers, and invest in security cameras. Consider investing in physical security of the building, possibly with the help of physical security consultant. **Responsibility:** IT manager, organization's management	the building where EPF office is located has an agreement with the Security Service of the Embassy that in case of necessity video materials of the Embassy Security Cameras will be exchanged. Two EPF office spaces are equipped with motion alarm system. In the case of an alarm, 4 people from the office receive a call and they can directly contact the Security of the building. A similar fire alarm system is installed for two offices.

Annex 2.4 IT Security Plan

On September 27, 2020, the Azerbaijan - supported by the Turkish military and Syrian mercenaries - started large scale military offence against the unrecognized Republic of Nagorny Karabakh. The 44 day-long armed conflict ended up with a Russian-brokered cease-fire on November 9, 2020, causing huge devastation to the region, left thousands dead, many settlements ruined, and a part of NK proper under Azerbaijani control. During the 44 days of armed conflict it was not safe to travel to the South of Armenia. As post-conflict demarcation of borders is not complete yet, South of Armenia remains a region of high security risk.

After the Velvet Revolution Armenia made progress in Internet freedom[2] reflected in Freedom House reports, at the same time a rise of hate speech and verbal assault is also recorded. Generally, civil society organizations are operating in relatively safe environment, however outspoken LGBT and feminist groups as well as human rights defenders are a subject to severe verbal attacks, predominantly online[3]. In 2019 one of the groups engaged in promulgation of anti-democratic values called 'Veto' for three consecutive weeks was blocking an entrance to theOpen Society Foundations-Armenia, after the 44-day armed conflict there were attacks on Radio Free Europe, OSF and some activists. There were also verbal attacks on EPF and its employees.

Post-conflict internal situation in the country remains tense. Anti-liberal, anti-democratic large- scale propaganda – both home grown and foreign baked- as well as unprecedentedly aggressive misinformation campaign is going on against various groups, especially against human rights defenders and peacebuilding community are at the target. On top of previous allegations, some activists are named 'traitors that have to be punished', foreign agents and 'spies of the enemy'. Among online verbal attacks trolling, dissemination of fake news, labelling and abusive media articles may be anticipated. From cyber-security perspective fishing of data, DDOS and virus attacks can be initiated.

In addition to the conflict, COVID-19 and imposed limitations, also impacted the overall securitysituation in the country. During the COVID-19-imposed lockdown (from April to July 2020), the activities under the "Partnership for Justice Reform" project were conducted on online working mode, which provided an opportunity to EPF and the Consortium members to conduct on-line discussions, training, involving also some stakeholders. Even after the post-pandemic period, EPF and its partners believe this modality of having joint online events/discussions, and trainingswill also continue.

The physical security of EPF premises is ensured through CCTV system and 24/7 security assurance. In compliance with EPF's policies and procedures, there is also a property insurance which covers physical damage to the space and equipment. EPF also has alarm system and will establish contact with the hot line of the Police covering the area. EPF will make sure that risky meetings are organized in safe spaces which already have security systems such as hotels, business centers, etc. As a part of DRL funded Partnership for Justice Reform project, EPF hired a team of psychologists who work with staff and partners providing counselling and support. Thepsychological assistance will be extended to other members of the team if needed.

EPF will share its Emergency Preparedness Plan (*Annex 18_EPF Emergency Preparedness Plan*), Incident Management Plan (*Annex 19_EPF Incident Management Plan*) and IT security and communication rules,

[2] https://freedomhouse.org/report/freedom-net/2018/armenia
[3] https://www.frontlinedefenders.org/en/location/armenia

which are part of EPF's Policies and Procedures (*Annex 17_EPF Armenia P&P Manual*), with other members of the Consortium.

The security plan of the project will anticipate the following activities:

1. For EPF staff travel to South of Armenia will be restricted and allowed only with writtenpermission of the CEO.
2. VPNs were set up for EPF, the messages are stored on ProtonMail servers in encrypted format. Secure implementations of AES, RSA, along with OpenPGP are used. The annualservice fee of the VPNs will be needed. EPF will provide additional VPN's to grantees and partners upon request.
3. Selection of the Facebook as a platform for online coordination/communication is determined not only by its large-scale usage but also security reasons. Facebook is more secure than any application developed and maintained locally. However, pro-bono onlineand cyber security trainings will be provided for partners and grantees.
4. Zoom platform is used for the online discussions and trainings. Security measures will betaken to ensure that personal data is protected, including setting passwords for all meetings and ensuring communication rules.
5. EPF will hire a high-level IT and cyber-security consultant for the entire course of theproject. The consultant will be responsible for ensuring IT and online security at the workplace and beyond for all Consortia members.
6. EPF will update its communications and public outreach strategies, taking into consideration recent cyber and physical attack risks.