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 Serious problems with EPF's 3 websites: epfarmenia am is an outdated Drupal installation on an Ubuntu 18.04 server, with an outdated version of php 7.2.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 management program to ensure that	**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.

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 usually closed for the outside world.	**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.

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 on local server. The data is encrypted and backed up on a

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	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 are no security cameras in and	**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 the building where EPF office is located has an agreement with the

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	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.