COMMITTEE MEETING

EB/CAM/20/9

October 12, 2020

To: Members of the Committee on Executive Board Administrative Matters

From: Gilles Bauche, Committee Secretary

Subject: **Proposed Information Security Framework of the Offices of Executive Directors**

Committee Action:	At the request of the Chairman, for **discussion** by Committee Members
Tentative Committee Meeting Date:	**Tuesday, October 20, 2020 at 10:00 a.m.,** via WebEx meeting.
Proposed Recommendation:	Pages 12-15
Questions:	Ms. Michaels, SEC (ext. 35451) Ms. Okutubo, ITD (ext. 39056) Mr. McDonald, ORM (ext. 37759) Mr. Plith, LEG (ext. 30562)
Additional Distribution:	Members of the Executive Board

INTERNATIONAL MONETARY FUND

PROPOSED INFORMATION SECURITY FRAMEWORK OF THE OFFICES OF EXECUTIVE DIRECTORS

October 12, 2020

Prepared by SEC, ORM, ITD and LEG Staff

This paper proposes an Information Security (IS) framework for the Offices of Executive Directors (OEDs). This framework is intended to address an important gap in the Fund's risk management architecture and IS perimeter, as identified in a third-party audit of the Fund's IS framework. Closing this gap is a milestone in ORM's "Information Security Roadmap" that was requested and endorsed by the Board.[1]

The proposals below are aligned in several important respects with the IS policies applicable to Fund staff, but have been tailored to the needs of the OEDs.[2] All Fund personnel have a collective responsibility to safeguard the Fund's information. Paragraph 10 of the Board Code of Conduct similarly requires Executive Directors to protect the security of any confidential information provided to, or generated by, the Fund.[3] However, as OEDs have a unique function as a channel of communications between the institution and member country authorities, they are a channel for sensitive communications coming into the Fund and for disseminating information outside the Fund. The proposed IS decisions for the OEDs seek to recognize this critical role and balance the operational needs of the OEDs with an appropriate risk mitigation mindset.

The proposed decisions focus on measures to protect the Fund's information networks from the risk of compromise, especially from external threats. Generally, the proposals aim (i) to ensure that OED personnel are aware of emerging threats, and understand their role in exercising due diligence against them, and (ii) to enable ITD to act to protect the network through appropriate measures. The specific measures outlined below would enable the OEDs to close the gap in the IS perimeter significantly, but do not fully address the issue of transmission of sensitive Fund information outside the Fund. As a second stage in this work, staff propose to consult further with the OEDs

[1] 2018 Risk Report, SM/18/246; The Acting Chairs Summing Up, SM/18/246.

[2] The Fund's Information Security Policies encompass a suite of six policies: Information Security Policy, Acceptable Use Policy; Access to Fund Information Systems Policy, Information Technology System Security Policy; Information Security Incident Management Policy: and the Supplier Security Policy.

[3] Compendium of Executive Board Work Procedures, Section 9.3 Code of Conduct for Members of the Executive Board, paragraph 264. The Executive Board adopted the code of conduct on July 14, 2000. It is also available on the Fund's external website.

on this remaining aspect of managing information security to understand their operational constraints better, before considering how to formulate additional proposals.

BACKGROUND

1. Fund Management has adopted IS Policies in order to protect the security of the Fund's Information Assets from both internal and external threats. The IS policies are predicated on the position that all information that Fund employees create, store, transmit or use in conducting the Fund's mission is the property of the Fund.[4] The Fund's IS policies detail appropriate procedures for the creation, maintenance and dissemination of Fund Information Assets, alongside operational standards for conducting the business of the Fund. In doing so they aim to:

I. Align IS risk assessment with the risk acceptance level of low endorsed by the Board;

II. Define accountability and responsibility for properly protecting Information Assets owned by the Fund to manage and mitigate information security risk[5];

III. Establish the necessary baseline security requirements to safeguard (ensuring the integrity, availability and confidentiality of) Information Assets to reduce business and legal risk and protect the reputation of the Fund; and

IV. Define consequences for non-compliance with these policies and related standards and procedures.

2. These policies have been approved by Fund Management and, as such, are not directly binding upon Offices of Executive Directors (OEDs). New Executive Board decisions are required to establish an appropriate IS framework for the OEDs. The Fund's IS Policies applicable to staff provide a good basis for defining best practices that could also be adopted by the OEDs; however, the staff policies encompass several elements that are not directly relevant to the OEDs (including the mechanisms for managing any disciplinary actions arising from serious breaches of these policies that may constitute misconduct under the Staff Handbook).

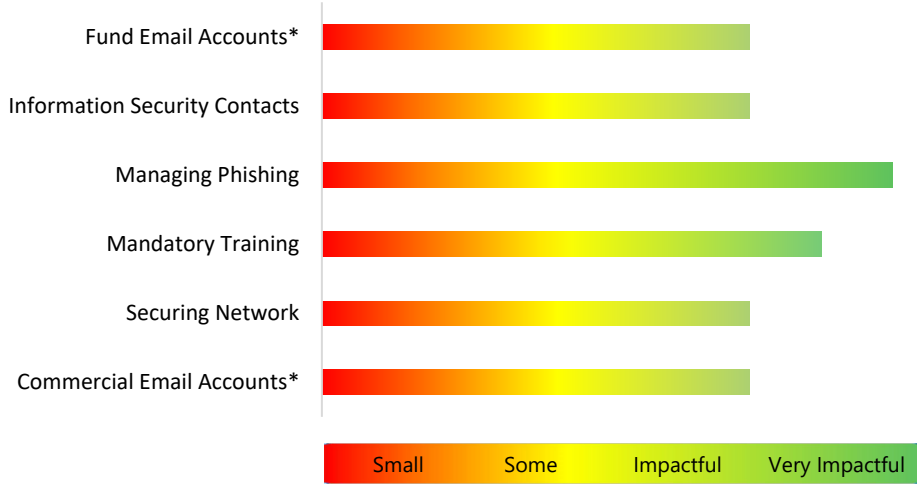
3. Rather than apply the staff policies selectively, for transparency and clarity it is proposed that the CAM recommend that the Executive Board adopts separate IS decisions for the Offices of Executive Directors. The decisions outline specific responsibilities of the personnel elected or appointed to positions in the OEDs for ensuring that they understand their responsibilities, and fulfil their obligations, for maintaining the security of the Fund's information assets. These decisions would also authorize management to act to protect the network through

[4] Information that is private and personal in nature, but saved on Fund-issued devices and approved personal devices used for Fund business, is included under the definition of Information Assets.

[5] Information Asset includes all forms of hard copy and of electronic materials, wherever they are located, whatever the sort of information they contain, whatever the medium in which information is stored (including audio and video material), and whatever their purpose.

appropriate measures. The proposed measures would be significant steps towards strengthening the Fund's IS posture, as shown in Figure 1.

Figure 1. Information Security Risk Mitigation: Estimated Individual Risk Reduction Impact of Adopting Proposals



*Assessment assumes OEDs' remain vigilant to risks associated with use of these accounts and exercise heightened caution in using them.

PROPOSED OED INFORMATION SECURITY FRAMEWORK

4. As noted above, all Fund personnel—including the OEDs—have a collective responsibility to safeguard the Fund's information security. The strong support expressed in several Board discussions amply illustrates Executive Directors' commitment to this principle.

5. The Fund's information systems already deploy extensive automated protocols for detecting and mitigating risks. ITD estimates that over 71 million potentially malicious emails were successfully detected and blocked between August 2019 and July 2020. It is not enough, however, to place reliance on these mechanisms alone—the vigilance and care of Fund personnel, including OED personnel, are a critical element of the Fund's information security posture.

6. The proposals below seek to balance the need for strong institutional risk management with recognition of the operational realities of the OEDs. It is understood that OEDs must communicate extensively with their member countries, and many of those communications remain under the direct purview and authority of the Executive Director, including draft BUFF/ED or Gray statements, meeting notes, and other internal and informal documents. In general, the practice whereby Executive Directors share certain confidential information with the

authorities of members in their constituencies is not considered to be inconsistent with their duty of confidentiality. However, documents provided to national authorities on a confidential or restricted basis retain their confidential character, and authorities are obliged to ensure that the applicable Fund restrictions on access to these documents are respected.

7. It is proposed that the decisions set out below would apply to all personnel in an Office of Executive Director for whom information system access is granted. They would encompass direct employees (Executive Directors, Alternate Executive Directors, Senior Advisors to Executive Director, Advisors to Executive Director, Assistants to Executive Director, and contractual employees working in an OED) and also any non-remunerated personnel stationed in an Office of Executive Director but who are not directly employed by the Fund (e.g. government-provided personnel) for whom the host OED requests information system access.[6]

8. Specific decisions are proposed in the following areas:

(i) Responsibility to exercise due care;

(ii) Appointment of Information Security Contacts in each OED;

(iii) Mandatory participation in information security training;

(iv) Protocols for managing and reporting phishing risks;

(v) Requirement to use Fund email accounts to conduct official business operations;

(vi) Avoidance of transmission of Fund information via unsecured, commercial email accounts, except where such email accounts are the only mode of transmission available;

(vii) Actions to secure the Fund network against threats.

Exercise Due Care to Protect the Fund Network

9. It is important to be careful. As noted above, in addition to the extensive automated protection systems deployed by the Fund, there is a critical human element to the maintaining the security of the Fund information systems. All personnel, including OED personnel, shall:

- Not engage in inappropriate activities (disabling security controls or features, execution of programs, software, processes or automated transaction-based commands) that can potentially lead to an information security breach or directly cause a disruption or harm to the Fund's Information Assets;

[6] Visitors and interns are considered to be "observers", who are not present in an OED in a working capacity. Accordingly, these personnel are not granted information system access, but under their letters of invitation, they are required to maintain the confidentiality of Fund information at all times.

- Not share, provide or loan Fund-issued devices with Fund and non-Fund personnel in any circumstances, including to spouses and family members.

- Make every effort to protect login/sign on credentials and the associated passwords, PINS, tokens and other access devices from disclosure to others and from loss. Personnel must not share their password or other authentication credentials with anyone, including their manager, co-workers, family members, friends or technical support personnel.

Appointment of OED Information Security Contact

10. Maintaining an effective, open channel of communications to the OEDs on emerging information security risks will be an important step in building a shared understanding of these risks, and a collaborative engagement on how best to address them. To facilitate this ongoing dialogue, it is proposed that each OED designate a senior employee (Executive Director, Alternate Executive Director or Senior Advisor) as an Office Information Security Contact ("OISC"). This role would be equivalent to the Departmental Information Security Contacts appointed by each staff department.

11. The role of the OISCs would be to be provide a focal point for IS matters and facilitate implementation of good IS practices in their Offices. This measure allows for early notification of IS issues, a forum for engagement on issues of particular concern to the OEDs, and a point of contact for reporting on participation in mandatory IS training and security exercises as proposed below. The Secretary's Department would request these designations both in an initial phase and as any personnel transitions occur.

Mandatory Participation in Fund Information Security Training

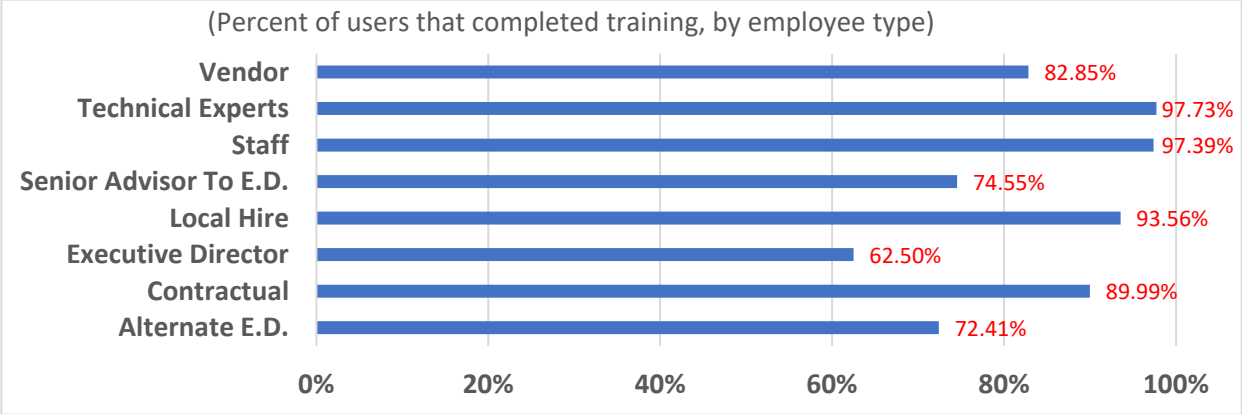
12. It is proposed that OED personnel be required to participate in the same IS training and Crown Jewels training that is required of Fund staff. These training courses are important for ensuring ongoing awareness of the responsibilities of all Fund personnel to protect Fund information, and be vigilant to IS threats. Historically, voluntary participation in this training by OED personnel has tended to be low (see Figures 1 and 2 below), but recent targeted communications to the OEDs from the ITD Director have increased participation levels over the past year. Completing this training as a condition of activating network access at the time of hire, and on an ongoing basis (i.e., refresher training) would close this gap fully. The OISCs could support follow-up by encouraging completion of periodic refresher training within their Offices. ITD will support these efforts by:

- Continuing to send reminders to OED personnel of the need to complete the training;

- Providing reporting on training completion (by OED) and secure user behavior to OISCs (i.e. statistics related to training, positive recognition of vigilant and cyber risk-aware personnel, phishing, information security incidents etc).

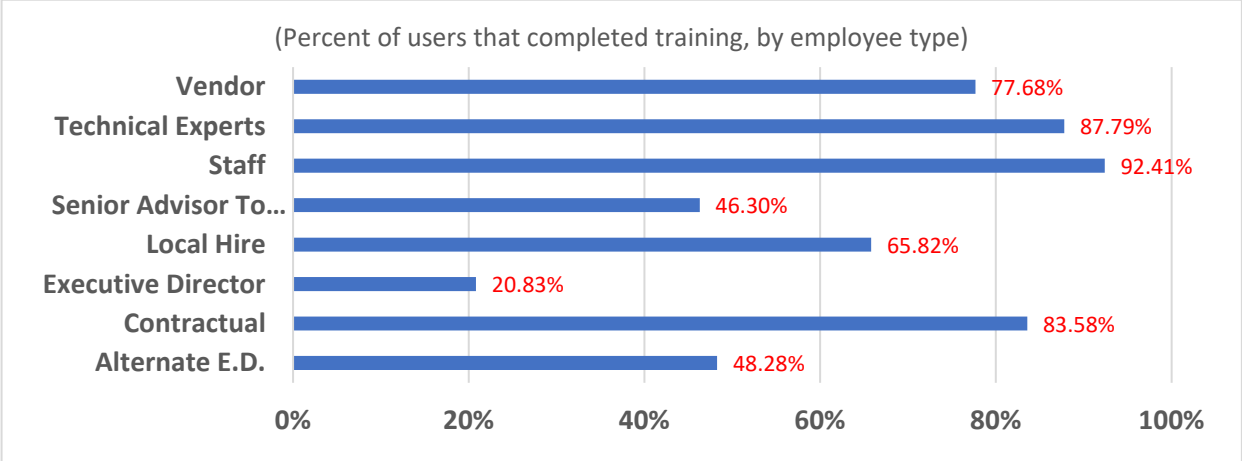
- Including information on OED Information Security training completion in aggregate reporting included in Fund-wide reporting on secure user behavior.

Figure 2. Annual Information Security Training Completion August 2020



Source: ITD

Figure 3. Safeguarding the Crown Jewels Training Completion August 2020

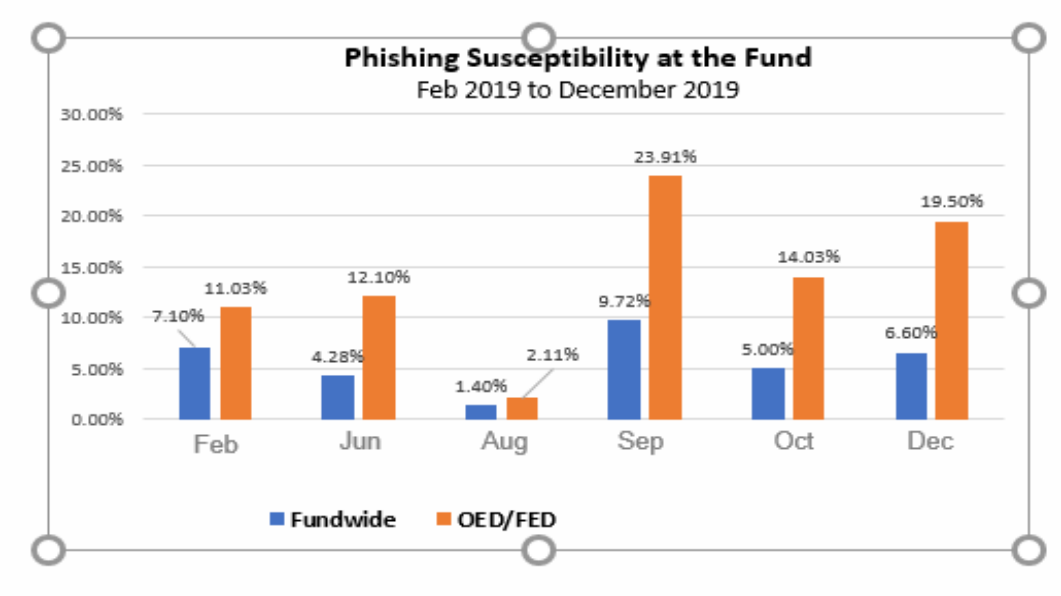


Source: ITD

Managing and Mitigating Phishing Risks

13. OED personnel should remain vigilant to attempts to compromise the security of Fund information systems through introduction of malware, including through phishing attacks. OEDs are routinely specific targets for phishing attacks. OED participation in regular information security training will help to raise awareness of, and to mitigate these risks.

Figure 4. Phishing Susceptibility at the Fund



Source: ITD

14. OED personnel should exercise all reasonable care to avoid opening malicious emails, attachments, and clicking on unknown links. It is proposed that, similar to the policies for Fund staff, the following protocol shall apply to OED personnel who open Fund IT security training phishing emails:

(i) For a first incident, the individual will be notified by the Information Technology Department (ITD) of the infraction and reminded of the need to be vigilant;

(ii) For a second incident, in addition to notification of the individual, the Executive Director shall also be notified (or, if the Executive Director fails a second phishing test, he/she will receive a second reminder);

(iii) For a third incident; in addition to notification of the individual and the Executive Director, the individual shall be required to take a refresher IS training within a reasonable timeframe on the same basis as is done for staff.

Use of Fund Email Account for Conduct of Business Operations

15. OED personnel, like Fund staff, should use their Fund official email accounts for the conduct of their work for the institution, including transmitting information to their member country authorities. Similarly, OED personnel should not use their personal email accounts to store

or back up of Fund information outside the Fund system, or other cloud-based solutions for this purpose (e.g. Dropbox, Google, etc.).[7]

Avoidance of Transmission of Fund Information via Unsecured, Commercial Email Accounts, Unless No Other Option is Available

16. Use of unsecured commercial email accounts (e.g. gmail and yahoo email accounts) presents risks to the institution. These accounts are more vulnerable to the risk of compromise.. Anyone can create such an account, and these accounts are more easily impersonated. Unlike official email accounts, the Fund's security system is unable to validate the identity of the individual sitting behind an unsecured commercial email account. The COVID-19 crisis has coincided with an increased incidence of attempts to compromise IMF information system security through impersonation of unsecured commercial email addresses. ITD is currently working to protect the Fund from incoming emails with attachments transmitted to Fund personnel from unsecured commercial accounts.

17. OED personnel should be aware of these risks, and avoid—wherever possible—sending Fund information to unsecured commercial email accounts used by member country authorities. It is recognized that some member country authorities use commercial email addresses extensively due to infrastructural limitations within those countries. OED personnel should only send information to commercial email accounts when it is the only practicable means of communication with their authorities. If no other option is available, OED personnel should exercise heightened caution in using these channels of communication. Staff will consult with OEDs during the second phase to further understand their operational constraints in this regard.

Securing the Fund Network Against Threats

18. Breaches of the Fund's information systems can occur unintentionally or intentionally, and the severity of a breach of the security system may also vary. In all situations, the institution's priority is to preserve the integrity and security of its information systems. Similarly, all personnel, including OED personnel, have a duty to exercise due care to protect the Fund's information security and report malicious activity to ITD. To this end, it is proposed that OED personnel, like Fund staff, would be required to:

- Exercise care when clicking on links and email attachments. If an email seems suspicious, OED Personnel must report it to virus@imf.org immediately.
- Promptly change their passwords and other authentication credentials in case of a suspected compromise and report it to the IT Help Desk.

[7] This includes home email accounts, cloud-based solutions, or professional accounts OED employees may continue to hold with their prior employer.

- Promptly report any observed/suspected information security event or incident (for example, unauthorized access to or misuse of Fund information or information systems, any actual, detected, or suspected virus-related problem, or weakness or vulnerability in the Fund's information assets) to the IT Help Desk.

- Promptly report lost, stolen or compromised Fund or personal mobile devices used to store or access Fund information to the IT Help Desk.

- Not attempt to resolve information security incidents by themselves.

- Treat information related to security incidents and unmitigated technology vulnerabilities as Strictly Confidential and only disclose such information to those who have a strict need to know.

19. It is proposed that the main features of the Fund's routine incident reporting, triaging, and system security protocols apply also to OED personnel. Annex 1 illustrates the reporting and triage measures applicable to Fund staff. It is proposed that the following steps are made applicable also to OED personnel:

- If a security event occurs on a Fund account or device held by an OED personnel, ITD will contact the user (or the user may self-report the event to the IT Helpdesk);

- ITD will collect the device and the user may request a loaner device from the IT Helpdesk. ITD will conduct an investigation to determine the impact of the security incident. If the investigation indicates no broader threat to the Fund's system, the device is returned to the user.

- If the investigation indicates potential Code of Conduct issues, in line with the provisions of the Executive Board Code of Conduct, ITD will refer the matter to the Executive Director or the Executive Board Ethics committee, as the case may be, for further action, as set forth in paragraph 24 below.[8]

20. It is proposed that, if an actual breach of the system is caused by OED personnel, intentionally or not, ITD should take its standard measures to preserve the security of the information system, including by shutting down system access immediately if such action is needed to mitigate risks to the Fund's information system. In these cases (which are expected to be rare), the Executive Director and the OED employee would be notified when the action is taken, and why it has been deemed necessary. The Executive Director would also be notified in the event that ITD suspends or terminates system access. In the event that ITD determines that managing IS requires suspending or terminating system access privileges[9], any request to re-instate privileges for a user account would need to be approved first by the Executive Director and then submitted to ITD.

[8] For staff, if ITD determines that a security incident may constitute misconduct, the matter is escalated to the Office of Internal Investigation (OII). If a forensic review by the OII confirms that misconduct has occurred, Fund management may take disciplinary actions up to, and including, termination of employment of the staff member.

[9] These provisions would also apply to requests by separating OED personnel to extend email account privileges for a maximum period of up to two weeks following departure from the Fund.

ITD will review the submission; if a determination is made user access can be reinstated without causing an unacceptable risk to the Fund's information system the user will have their privileges reinstated. In cases where risks to the Fund's information system remain, ITD will discuss these concerns with the Executive Director to seek resolution.

21. In cases where there is a serious IS breach by OED personnel that would likely amount to misconduct if committed by Fund staff, Management would notify the relevant Executive Director. As provided for in the Executive Board Code of Conduct, it would be the Executive Director's responsibility in the first instance to enforce these policies with her/his staff.[10] The referral of the matter to the Executive Director may include a request to grant permission for ITD to monitor Fund email, internet traffic, data files, and other network activity. If the Executive Director does not take appropriate steps to respond to the breach of a person in his/her office, or if the Executive Director is the source of the breach, then Management would report the alleged breach to the Executive Board Ethics Committee for consideration.[11]

COMPLETING THE INFORMATION SECURITY RISK PERIMETER

22. As noted above, the measures proposed in this paper focus on strengthening the OEDs' awareness and ability to respond to "in-bound" risks posed to the Fund's information security perimeter. Fully closing the IS perimeter would encompass the "outbound" transmission of sensitive Fund information to external parties outside the institution. The Fund currently deploys three secure platforms for transmitting highly sensitive information to external parties: (i) email encryption; (ii) secure transmission of Strictly Confidential and Confidential Fund documents to designated member country authorities via IMF Connect; and (iii) Box, a secure file sharing service. While OEDs should strive to transmit sensitive information to member country authorities via these secure platforms as much as possible, anecdotal evidence indicates that OEDs have found it difficult to deploy these tools efficiently and effectively.

23. This remaining risk area raises complex issues for the OEDs given the role of the OEDs as a channel of communication to their member country authorities. In its preparatory discussions on this issue, the CAM has noted several issues of concern to the OEDs: the risk of confidential correspondence between Executive Directors and their member country authorities becoming compromised; practical difficulties in transmitting sensitive Fund documents to the relevant officials in their member country authorities rapidly via available technology; and the risk of

[10] Paragraph 3 of the Board Code of Conduct states that "Executive Directors are responsible for considering any allegations of misconduct …in their respective offices and should take such measures as are necessary and appropriate in the circumstances".

[11] An Executive Directors' failure to act could give rise to an allegation against him/her under paragraph 7 of the Code of Conduct (Executive Directors have an "obligation to exercise adequate control and supervision over matters for which they are individually responsible") and as the Ethics Committee oversees the Executive Directors pursuant to paragraph 24 of the Code of Conduct, an allegation of misconduct by an ED should go directly to the Ethics Committee.

classified Fund documents potentially being misused. The latter two issues are matters of particular concern with regard to Fund documents classified as Strictly Confidential or Confidential, in accordance with frameworks approved by management and the Executive Board.

24. Before considering these issues further, the CAM recommends that ITD and SEC consult bilaterally with the OEDs to inform them of the variety of tools that are available, and gain an understanding of any operational difficulties and impediments that they are experiencing with these tools. The appointment of OED Information Security Contacts will facilitate this dialogue. The CAM could further consider the need for additional information security policies, and/or best practices, taking this consultation into account.

25. The CAM therefore recommends that the measures proposed in this paper should be adopted now, as a strong first step towards closing the gap in the IS perimeter and to provide a platform for further engagement on remaining risks. The proposed measures lower the risk gap to an acceptable level, pending completion of further work to determine best practices for OED communications with their member country authorities.

Proposed Recommendation

The CAM recommends the following decision for adoption by the Executive Board:

(i) **The decisions set forth below in paragraphs (ii) to (ix) shall be applicable to all personnel in the Offices of Executive Directors (OEDs)**, including Executive Directors, Alternate Executive Directors, Senior Advisors and Advisors to Executive Directors, Assistants to Executive Directors, contractual personnel employed in the OEDs, and Government-Provided Personnel who are stationed in OEDs. Non-remunerated visitors to OEDs, who are not provided with access to the Fund's information system, shall be required at all times to safeguard the confidentiality of Fund information assets.

(ii) **Exercising due care to protect the Fund's information security and information assets: In order to protect the Fund's information systems, OED personnel shall:**

- Make every effort to protect login/sign-on credentials and the associated passwords, PINS, tokens and other access devices from disclosure to others and from loss. OED Personnel must not share their password or other authentication credentials with anyone, including their manager, co-workers, family members, friends or technical support personnel;
- Exercise care when clicking on links and email attachments. If an email seems suspicious, OED Personnel shall report it to virus@imf.org immediately;
- Promptly change their passwords and other authentication credentials in case of a suspected compromise and report it to the IT Help Desk;
- Promptly report any observed/suspected information security event or incident (for example, unauthorized access to or misuse of Fund information or information systems, any actual, detected, or suspected virus-related problem, or weakness or vulnerability in the Fund's information assets) to the IT Help Desk;
- Promptly report lost, stolen or compromised Fund or personal mobile devices used to store or access Fund information to the IT Help Desk;

- Treat information related to security incidents and unmitigated technology vulnerabilities as Strictly Confidential and only disclose such information to those who have a strict need to know.

OED personnel shall not:

- Engage in inappropriate activities (disabling security controls or features, execution of programs, software, processes or automated transaction-based commands) that can potentially lead to an information security breach or directly cause a disruption or harm to the Fund's Information Assets;
- Share, provide or loan Fund-issued devices with Fund and non-Fund personnel in any circumstances, including spouses and family members; or
- Attempt to resolve information security incidents by themselves.

(iii) **Mitigating Phishing Risks:** OED personnel shall remain vigilant at all times to attempts to compromise the security of Fund information systems through introduction of malware, including phishing attacks, and shall exercise all reasonable care to avoid opening malicious emails, attachments, and clicking on unknown links. The following protocol will apply to OED personnel who open Fund IT security training phishing emails:

- For a first incident, the individual will be notified by the Information Technology Department (ITD) of the infraction and reminded of the need to be vigilant;
- For a second incident, in addition to notification of the individual, the Executive Director shall also be notified (or, if the Executive Director fails a second phishing test, he/she will receive a second reminder);
- For a third incident; in addition to notification of the individual and the Executive Director, the individual shall be required to take refresher IS training within a reasonable timeframe on the same basis as for staff.

(iv) **Appointment of OED Information Security Contacts:** Each OED shall appoint a senior employee (Executive Director, Alternate Executive Director or Senior Advisor) as an Office Information Security Contact ("OISCs"). The designated OISCs shall act as a focal point for

information security matters and facilitate implementation of defined information security practices in their Offices.

(v) **Participation in Information Security Training:** All OED personnel shall complete the same Fund Information Security training required of Fund staff, as a condition of being provided access to the Fund email and network systems on entry on duty, and shall be required to complete periodic refresher training thereafter on the same basis as Fund staff. This responsibility cannot be transferred.

(vi) **Use of Fund Email Account for Conduct of Business Operations:** OED personnel shall use their Fund official email accounts when conducting Fund related business in accordance with their job responsibilities. They may not store or back up Fund information on non-Fund email accounts or other non-Fund repositories e.g. Drop-box, Google Drive, etc.

(vii) **Avoidance of Transmission of Fund Information to Unsecured Commercial Email Accounts:** OED personnel shall not transmit Fund information to unsecured commercial email accounts unless no other option is available. In these circumstances, OED personnel shall exercise heightened caution in using these unsecured channels of communication in order to avoid unauthorized disclosures of Fund information.

(viii) **Managing Information Security Incidents:** In the event of a breach of the Fund's information security by or via any OED personnel, ITD is authorized to take measures to preserve the security of the IT system, including by shutting down IT system access immediately if such action is needed to mitigate risks. In such cases, the Executive Director and OED personnel shall be notified as soon as possible of the action taken and the basis for it. The Executive Director would also be notified in the event that ITD suspends or terminates system access. If ITD determines that managing Fund IS requires suspending or terminating system access privileges, any request to re-instate privileges for an OED user account would need to be approved first by the Executive Director of the Office and then submitted to ITD. ITD will review the submission; if a determination is made user access can be reinstated without causing an unacceptable risk to the Fund's information system the user will have their privileges reinstated.

(ix) **Investigation of Possible Misconduct:** Where there is an allegation of a serious breach of the Fund's information systems by OED personnel, that, if the allegation had concerned Fund staff, would have generated an investigation into misconduct, Management shall raise the issue with the relevant Executive Director. The referral of the matter to the Executive Director may include a request to grant permission for ITD to monitor Fund email, internet traffic, data files, and other network activity. Where an Executive Director does not take appropriate steps to respond to a serious breach of the Fund's information security by a person in his/her office, or if the Executive Director is the source of the breach, then Management shall report the alleged breach to the Ethics Committee for consideration.

Annex I. IT Risk Management Protocols for OEDs