

Information Security Policy for Contractors

AMS 6.20G
Last Updated: May, 2016

1. Policy

1.1. Policy Rationale

This policy establishes basic principles and requirements for Contractors necessary for the secure use and management of the World Bank Group's ("Bank Group" or "WBG") information and information systems.

1.2. Applicability

This policy applies to all Contractors, on-site and offshore, at all locations throughout the world that are using Bank Group systems or accessing, processing, or storing Bank Group Restricted Information, as per [The World Bank Policy on Access to Information](#) Policy, whether in electronic format or otherwise.

2. Written Information Security Program (WISP)

2.1. Contractors must implement and maintain a written information security program applicable to the Contract, which, at a minimum, accomplishes all of the following:

- Designates an Information Security Officer, which may be any employee with sufficient authority and experience to implement and maintain the written information security program;
- Provides for regular training of all Contractor and Subcontractor employees on appropriate security procedures and techniques;
- Provides common industry security practices and controls including AV/Malware protection;
- Requires the performance of an initial and annual assessment of Contractor's security vulnerabilities;
- Requires that Contractor implement appropriate safeguards to address any security vulnerabilities;
- Requires the implementation and annual review of an incident response plan;
- Requires the performance of an annual review of the written information security program;
- Implements a process for evaluating and auditing the ability of all Subcontractors to meet the same security requirements that Contractor must meet; and
- Establishes secure protocols for user authentication and user access to Bank Group information and systems.

2.2. The WISP is subject to review and approval by the WBG Office of Information Security.

3. Internal Service Providers

3.1. Internal service providers are Contractors, offsite or on Bank Group premises, that access WBG systems and information directly through the WBG network or via authorized remote connection

to the WBG network. This would include Contractors working from one of Bank Group's offshore development centers (ODCs).

3.2. Information Security Training

- 3.2.1. All Contractor and Subcontractor employees with access to Bank Group systems or Bank Group information must complete the mandatory information security e-learning course to ensure that they fully understand their responsibilities for protecting the World Bank Group's information when provided with access privileges. Such employees must receive training on appropriate security policies and procedures on a periodic basis as decided by the Office of Information Security. Failure to comply may result in access revocation.

3.3. Information Assets and User Access

- 3.3.1. All Bank Group information assets (e.g. data, databases, reports, communications, manuals, documentation for systems, procedures, and plans) are considered "Confidential", unless expressly stated otherwise by the information provider.
- 3.3.2. Contractors are responsible for protecting all Bank Group information and the systems which process, store and transmit such information from unauthorized disclosure and modification regardless of location. Contractors which will be using or accessing the International Finance Corporation's ("IFC's") systems, information, electronic or otherwise must abide by all relevant IFC specific policies and procedures including the IFC Policy on Disclosure of Information. Contractors must ensure that all of their staff or subcontractor staff who use or access IFC systems or information abide by such IFC policies and procedures. If there are differences between IFC policies and procedures and those in other World Bank Group policies and procedures, the IFC policies and procedures shall apply where IFC systems or information are being accessed or used.
- 3.3.3. Contractor and Subcontractor access rights shall be determined by the Bank Group Project Manager. Contractor and Subcontractor employees shall be granted the least amount of access to Bank Group systems and information necessary for such employees to perform their contractual functions. Any unauthorized attempt to access information that is outside the access parameters set by the Bank Group Project Manager is prohibited.
- 3.3.4. Contractors shall not, unless expressly authorized by the Office of Information Security (OIS) in writing, connect non-standard hardware, or personal devices to the World Bank Group's network.

3.4. User Credentials

- 3.4.1. User credentials are provided to Contractors by WBG to facilitate their work functions as defined in the contract. Credentials include, but are not limited to: username, password, Multi-Factor Authentication token, and physical access badge.
- 3.4.2. Each Contractor is responsible for safeguarding his or her credentials, and protecting them from unauthorized use.
- 3.4.3. Contractors are prohibited from disclosing or sharing their credentials with others.
- 3.4.4. Contractors are accountable for any incident arising from improperly protected credentials. Compromised credentials must be immediately reported to the Project Manager and changed or invalidated.
- 3.4.5. Any unauthorized attempt to discover or obtain the credentials of another user or to access Bank Group information or systems using another person's credentials is prohibited.
- 3.4.6. All passwords used to access Bank Group Systems must meet the following criteria:

- Passwords must be at least 8 characters in length, they must be sufficiently complex that they cannot be easily guessed, and they must use both alphanumeric and special characters;
- Passwords must be changed every 90 days;
- Users shall not repeat any of his or her last 5 passwords;
- Upon receiving access credentials, users shall immediately change the password to a unique value known only to the user;
- Users shall not rely on default passwords;
- Contractor shall prohibit users from sharing passwords with anyone; and
- Contractor shall prohibit users from recording passwords on paper or in a document.

3.5. Information Systems Use

- 3.5.1. All Bank Group information systems (i.e. email, internet, telephones, fax, etc.) are the property of the Bank Group and are primarily for Bank Group business use. Contractors may use them for incidental personal purposes, as defined by the Acceptable Use Policy, and must never use them to knowingly access, store, or distribute pornographic or otherwise offensive or illegal material. Contractors may not use Bank Group systems to knowingly compromise other Bank Group systems, networks or safeguards.
- 3.5.2. Contractor personnel shall not install, modify, or uninstall software on any device that is used to access the Bank Group systems or Bank Group information without the explicit authorization of the Project Manager.
- 3.5.3. Contractor's computers, laptops, smart phones, and other devices or portable media assigned by the Bank Group and/or containing Bank Group information must be secured by their users from theft and unauthorized use and may not be left unattended in a public space, including in a personal vehicle.
- 3.5.4. Contractors may not leave unattended in a non-public space any device containing Bank Group information unless a password-enabled locking mechanism is engaged.
- 3.5.5. To ensure information security and integrity, Contractors must always completely log out from all applications, leave desktop computers in a locked state, turn off peripheral devices, and lock cabinets and other information storage containers when left unattended.
- 3.5.6. All systems and software packages must be fully tested for system compatibility and for the presence of malicious code and covert channels by the Office of Information Security (OIS) before installation and use.
- 3.5.7. Contractors may not remove equipment from Bank Group facilities without explicit authorization from the Project Manager.
- 3.5.8. Contractors must always backup critical electronic files to an appropriate network drive as authorized by the Project Manager.
- 3.5.9. Contractors must ensure that all information is removed from devices or storage containers that are moved off-site and are no longer under their direct control. If in electronic format, information must be overwritten, not just deleted. Contractors must provide the Bank Group with a documented process for information removal/destruction and written verification of specific implementation of this process as it relates to the subject contract.

3.6. Encryption

- 3.6.1. Contractors shall use encryption to protect all Bank Group information from inadvertent disclosure when such information is sent over the Internet or other open, non-Bank Group networks. Such encryption must meet industry standards.
- 3.6.2. Contractors shall use encryption whenever possible when transmitting Bank Group information within the Bank Group network.
- 3.6.3. Contractors are prohibited from removing any information from the Bank Group network unless strictly necessary to perform a function under its contract and authorized by the Project Manager. Any information that is not stored on the Bank Group network must be encrypted and must be stored on a network that meets the standards set out in Section 4: External Service Provider Requirements.

3.7. Malicious Code

- 3.7.1. Contractors must use up-to-date malicious code protection (including anti-virus) software for all systems and devices that are used to access Bank Group systems or Bank Group information.
- 3.7.2. Contractors are prohibited from introducing malicious code into Bank Group systems, software, or devices.
- 3.7.3. Contractors are prohibited from attempting to bypass Bank Group malicious code protection software or other system safeguards (e.g. when downloading or transferring information).
- 3.7.4. Contractors must always use installed Bank Group malicious code protection software and other system safeguards. Contractors must scan all files and software before introducing them to Bank Group systems.

3.8. Incident Reporting

- 3.8.1. All information security incidents (e.g. malicious code, worms, viruses, unauthorized or inappropriate email/internet use) must be immediately reported to the Global Support Center and Project Manager upon discovery. In no event shall Contractor take longer than 24 hours to report a security incident.
- 3.8.2. Loss of Bank Group assigned desktop, portable, or mobile computing devices by any means (e.g. theft, loss, breakage) must be reported to the Global Support Center and Project Manager as soon as discovered.

3.9. Telecommunications Security

- 3.9.1. Contractors are responsible for being aware of current and potential telecommunications (e.g. telephones, voice mail, mobile phones, conference calls, instant messaging, and facsimile machines) security risks in their given environment, and must always consider information sensitivity and transmission security issues when selecting a communications medium.

3.10. Remote Access

- 3.10.1. Remote access refers to Contractors using telecommunications/remote access to conduct their authorized activities from a location other than WBG networks.
- 3.10.2. All Bank Group-owned desktop, portable or mobile computing devices must employ access control and user authentication mechanisms that have been approved by the Project Manager for access to the Bank Group's network.

- 3.10.3. For remote access using non-Bank Group owned computing devices, access will be controlled through an access account, the granting of which will be coordinated by the Project Manager. All non-Bank Group owned computing devices that are granted access to Bank Group systems must comply with all security requirements set out in this policy.
- 3.10.4. Authentication and information transmitted during a remote access session must be encrypted end-to-end and the session must be terminated when work is completed or when the remote access device will be left unattended.

4. External Service Provider Requirements

- 4.1. An External Service Provider (ESP) is a Contractor that hosts, stores, and/or processes Bank Group information and/or applications off Bank Group premises.

4.2. Pre-Engagement Requirements

- 4.2.1. The ESP must provide an overview of their information security management system including information security policies to the Project Manager for Bank Group review prior to the engagement.
- 4.2.2. The ESP must provide the Bank Group with an audit report of their information security management system conducted by a certified auditor when requested by the Bank Group.
- 4.2.3. A Service Level Agreement must be part of the contract between the ESP and the Bank Group.
- 4.2.4. The ESP must assign a single point of contact for the resolution of information security related issues and must notify the Sponsoring Business Unit and the Bank Group's Office of Information Security (OIS) in writing.

4.3. Personnel Requirements

- 4.3.1. All Contractor and Subcontractor personnel with access to Bank Group information, regardless of the location where such information is maintained, must complete the information security training requirements or equivalent identified above.
- 4.3.2. Any change in operational or security administration personnel assigned to Bank Group information systems must be communicated to the Sponsoring Business Unit and the OIS in writing.
- 4.3.3. The ESP must disclose who among its personnel and/or personnel of other entities will have access to the environment hosting the Bank Group's information or systems.
- 4.3.4. No Bank Group staff other than those authorized by the Sponsoring Business Unit should be given access to Bank Group information and systems.

4.4. Subcontractor Requirements

- 4.4.1. Before providing a subcontractor with access to Bank Group information, the ESP must ensure that all subcontractors and/or third parties engaged in the fulfillment of its contract with the Bank Group are aware of and agree in writing to adhere to all provisions contained in this Bank Group policy.
- 4.4.2. ESP must maintain a network monitoring capability along with appropriate user authentication procedures that will allow it to identify when a subcontractor has accessed the ESP's systems and what information the subcontractor accessed.

4.4.3. ESP must ensure that the subcontractor maintains an environment with equivalent or higher controls, policies and procedures than those applicable to ESP.

4.5. ESP Communications and Operations Security

4.5.1. On notification from the Sponsoring Business Unit, the ESP must be able to immediately disable all or part of the functionality of the application or systems should a security issue be identified.

4.5.2. The ESP must employ up-to-date malicious code protection software or systems to ensure the confidentiality, integrity, and availability of Bank Group information and information systems.

4.5.3. The ESP's System Administrators must maintain complete, accurate, and up-to-date information regarding the configuration of Bank Group hosted systems. This information must be made available to designated Bank Group personnel upon request.

4.5.4. The ESP must have a patch management process that includes the testing of patches before installation on Bank Group systems and on any ESP systems that host Bank Group information. Patch notifications must be communicated to the Sponsoring Business Unit.

4.5.5. The network hosting Bank Group applications must be logically isolated and/or segmented, separating the Bank Group systems network from other networks or customers that the ESP may have.

4.5.6. Host and network intrusion detection must be employed by the ESP where Bank Group systems are located. The ESP must also use data loss prevention software on any systems that host or have access to Bank Group information.

4.5.7. The ESP must subscribe to vulnerability intelligence services or to Information Security Advisories and other relevant sources providing current information about system vulnerabilities.

4.5.8. All changes to system configurations, services enabled, and permitted connectivity must be logged and the logs must be retained for a Bank Group prescribed period.

4.5.9. All system and user activities, including the ones which might be an indication of unauthorized usage or an attempt to compromise security measures must be logged for systems that process or store Bank Group information.

4.5.10. ESP must block access to any account following 5 failed log-in attempts. Access may not be restored until ESP security personnel have confirmed the identity of the user and the user's access privileges.

4.5.11. For all Bank Group applications and systems running Bank Group applications, log files must be protected to ensure confidentiality and integrity.

4.5.12. The Bank Group reserves the right to periodically audit the ESP to ensure compliance with the Bank Group's security policy and standards.

4.5.13. The ESP must perform daily backups of Bank Group information and systems, and safeguard all backup media.

4.5.14. The ESP must be able to adhere to Bank Group's data retention requirements.

4.5.15. The ESP must perform periodic tests on its control environment and provide 3rd party attestations to the Bank Group upon request.

5. Procedures

Access to procedures are available on a need-to-know basis. For access, contact the OIS.