
# Information Security Requirements for Contractors

## CONTENTS

## 1. PURPOSE AND APPLICATION

1.1 The purpose of this Standard is to establish the requirements for Contractor Employees accessing WBG Institutions and its Information and Technology Services.

1.2 This Standard applies to all Contractors with access to WBG Institution Information and Technology Services (or facilities processing or storing WBG Institution Information and Technology Services), and in accordance with the relevant business, contractual, information security, and institutional requirements.

## 2. DEFINITIONS

As used in this Standard, the capitalized terms and acronyms have the meanings set below:

a. **Authentication**: Is the process of verifying the identity of an individual or a device based on submitted Credentials.

b. **Authorization**: The process of granting access rights to a User, device, or program.

c. **Availability**: Relates to the business need to ensure that Information is available to authorized Users when required.

d. **Change Management**: The process for controlling the lifecycle of all Changes and enabling Changes to be made with minimum disruption to IT Services

e. **Contractor**: Means a company, organization, or a separate entity, such as an affiliate, division, or plant, that performs services and or supplies goods under contract to the WBG Institutions.

f. **Contractor Employee:** Anyone who performs services for WBG Institutions under a contract with a WBG Institution vendor.

g. **Credential:** An object or Information that is presented for verifying an individual or a device in an Authentication process.

h. **Encryption:** The process of encoding messages or Information in such a way that only authorized parties can read it.

i. **Information Security:** The process by which OIS protects the Confidentiality, Integrity and Availability of Information throughout its lifecycle.

j. **Logging:** The process of recording transactions or Events that occur on WBG Institution systems.

k. **Malware:** Any software designed to damage, disrupt or do other harmful actions on a computer system.

l. **Mobile Device:** A handheld portable computing device such as a smartphone or a tablet which has an operating system capable of running mobile apps.

m. **Monitoring:** The process of observing activities and performance of Information Systems to detect possible compromise, attack, or misuse.

n. **Network:** A number of systems that work together and between each other to achieve an overall objective.

o. **OIS:** Office of Information Security

p. **Passphrase:** A string of characters or a phrase that is part of the login Credentials and allows access to a computer, interface, system, or a data resource.

q. **Project Manager:** WBG Staff who supervises and coordinates activities with the Contractor.

r. **Subcontractor:** A company, organization, or a separate entity, such as an affiliate, division, or plant, that provides services to contractors.

s. **User:** Any person with access to any Information and Technology Services.

t. **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

u. **Vulnerability Management:** The management and remediation of system, infrastructure and Network Vulnerabilities.

v. **World Bank Institutions ("WBG Institutions"):** The collective identity of the International Bank for Reconstruction and Development (IBRD), the International Development Association (IDA), the International Finance Corporation (IFC), the Multilateral Investment Guarantee Agency (MIGA), and the International Centre for Settlement of Investment Disputes (ICSID).

w. **WBG Information and Technology Solutions ("WBG ITS"):** The Vice-Presidential Unit responsible for delivery of Information and Technology Services to the WBG Institutions.

## 3. REQUIREMENTS

**Contractor Information Security Requirements**

3.1 Contractors are responsible for ensuring that their employees and subcontractors adhere to all contractual requirements.

3.2 Conduct the business of WBG Institutions using Information Technology Services approved by WBG ITS.

3.3 Be accountable for all activities performed while using WBG Information and Technology Services.

3.4 Adhere to WBG's information classification and retention requirements.

3.5 Restrict the use of WBG Information and Technology Services to authorized WBG business-relevant activities.

3.6 Not test, explore, disable, or otherwise attempt to compromise any WBG Institutional Information Security controls, whether internal or external, unless authorized explicitly under operational or systems development requirements.

3.7 Complete all mandatory Information Security awareness training within established deadlines.

3.8 Immediately report any suspected or actual misuse of Information and Technology Services, Security Incidents impacting WBG Information or Systems, and other violations to designated WBG Institution contacts and OIS within 48 hours.

3.9 Loss of World Bank assigned desktop, portable or mobile devices by any means (i.e. theft, loss, breakage) must be reported to the defined WBG Institution contacts and OIS as soon as discovered.

3.10 All materials, files, information, software, devices, and other content, including personal information, transmitted, received, or stored by any WBG Institution using Information and Technology Services is treated and controlled as the property of that WBG Institution in accordance with its Policies, Directives and Procedures. This includes desktops, laptops, smartphones, and tablets provided to Contractor Employees.

3.11 Contractor Employees are not guaranteed privacy while using Information and Technology Services of the WBG Institutions.

**Personnel Security**

3.12 Adhere to the background check and verification process for Contractor Employees.

3.13 Comply with all onboarding and offboarding requirements and controls.

**Contractual Terms**

3.14 Communicate any relevant operational or security administration personnel change to the Sponsoring Business Unit and OIS promptly.

**Vendor Management**

3.15 Notify WBG Institutions of relevant subcontractors who have access to WBG Information or Systems.

3.16 Include Information Security requirements in contracts with relevant WBG Institution subcontractors.

3.17 Perform Information Security assessments of subcontractors.

3.18 Ensure that the subcontractor maintains an environment with equivalent or higher Information Security controls than those applicable to the contractors.

**Business Continuity / Disaster Requirements**

3.19 Document and share the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), where applicable, to ensure that essential business functions continue to operate during and after a disaster.

**Contractor Information Security Program**

3.20 Contractors must implement and maintain a formal Information Security program, which at a minimum accomplishes the following:

a. Implements common Information Security industry best practices and controls;

b. Requires the performance of an annual review of the Information Security program;

c. Requires the performance of an initial and annual assessment of the Contractor's security vulnerabilities;

d. Requires that Contractor implement appropriate safeguards to address any security vulnerabilities;

e. Requires the implementation and annual review of an incident response plan;

f. Implements a process for evaluating and auditing the ability of all Subcontractors to meet the same security requirements that the Contractor must meet;

g. Establishes secure protocols for user Authentication and user access to Work Bank information and systems; and

h. Provides for regular training of all Contractor and Subcontractor employees on appropriate security procedures and techniques.

**Physical Access to WBG Institution Facilities**

Information Security requirements for Contractors having physical access they will have to WBG Institution facilities:

3.21 Only access secure areas relevant to the Contractor's role.

3.22 Utilize badges and ensure they are always visible when present at WBG Institution facilities.

3.23 Secure physical documents and devices accessing WBG Institution Information from unauthorized use or theft (i.e., locked storage spaces, password-protect devices, etc.)

3.24 Not remove WBG owned equipment from facilities without written Authorization.

**Logical Access to WBG Information Technology and Services**

The following table defines Information Security requirements for Contractors based on the type of logical access they will have to WBG Institution Information and Technology Services. Requirements are classified into the following two scenarios:

a. ***Logical access via WBG Institution Devices*** (i.e., WBG Institution provided desktops and laptops, Firm-issued Mobile Devices, WBG Institution managed virtual machines).

b. ***Logical access via non-WBG Devices*** (i.e., contractor provided or personal laptops, personal Mobile Devices).

| Requirements | Logical Access | |
|---|---|---|
| | Applicable to WBG Institution Devices | Applicable to non-WBG Institution Devices |
| **Access Management** | | |
| 1.1. Adhere to WBG Institution access management processes. | ✓ | ✓ |
| 1.2. Safeguard Credentials and protect them from unauthorized use. | ✓ | ✓ |

| | | |
|---|---|---|
| 1.3. Create Passphrases with complexity (i.e., aging, alphanumeric, length) in line with the classification of the relevant System or entitlement and incompliance with WBG requirements. | ✓ | ✓ |
| **Information and Asset Handling** | | |
| 1.4. Install or use unlicensed software, that is not licensed to a WBG Institution or software not certified by WBG ITS for any purpose. | ✓ | |
| 1.5. Remove Information and Technology Services provided upon the completion of the Contractor's term of employment | | ✓ |

## 4. ROLES AND RESPONSIBILITIES

4.1 Contractors are responsible for:

a. Adhering to the requirements defined in this Standard.

4.2 Project Managers are responsible for:

a. Overseeing and Monitoring Contractor activities.

b. Escalating incidents related to Information Security and misuse of WBG Information and Technology Services.

c. Determining the appropriate access rights for Contractors for Information and Technology Services and approving access and permissions for use.

d. Coordinating the process of granting access account to contractors using non-WBG managed devices.

4.3 OIS is responsible for:

a. Defining Information Security requirement for Contractors to appropriately secure WBG Institutions Information and Technology Services.

4.4 Contract Manager is responsible for:

a. Ensure Information Security requirements are included in contracts with Contractors.