Information Security Policy for Contractors

10 September 2005

ISG Quality Program

Information Security Management System

Infrastructure Management System

Electronically distributed, subject to user discretion when printed.
Use the current version as in IRIS.

Table of Contents

Policy Rationale

1. This policy establishes basic principles necessary for the secure use and management of the World Bank Group's information and information systems.

Applicability

2. This policy applies to all Contractors at all locations throughout the world that are using Bank Group systems or accessing Bank Group information, electronic or otherwise.

Information Assets and User Authorization

3. 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 Bank Group's Project Manager in writing.

4. 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.

5. The Bank Group Project Manager is responsible for determining the access rights to information and systems and for granting Contractors appropriate access and permissions of use.

6. Contractors must lock filing cabinets and other storage receptacles containing Bank Group information when left unattended.

Information Systems Use

7. 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 and must never use them to knowingly access, store, or distribute pornographic or otherwise offensive material. Contractors may not use Bank Group systems to knowingly compromise other Bank Group systems, networks or safeguards.

8. Contractors are expected to make every effort to ensure that all Bank Group information is protected from inadvertent disclosure when being sent over the Internet or other open, non-Bank Group networks. Encryption or password protection must be used when available to protect Bank Group information. If unable to encrypt, Contractors should consider alternatives to email for transference. When transmitting within the Bank Group network, encryption is available through active steps in Lotus Notes. For communications outside of the Bank Group's network, the Information Solutions Group can provide options and methods of encrypting information.

9. Any unauthorized attempt to access information that is outside the Contractor’s “need-to-know” for his/her operational purposes is prohibited.

Passwords and User IDs for Accessing Bank Group Systems

10. Each Contractor is responsible for safeguarding his or her password, user ID, and badge, and protecting them from unauthorized use.

11. Contractors are prohibited from disclosing or sharing passwords or user IDs with others.

12. Contractors are accountable for any incident arising from improperly protected personal user IDs and passwords. Compromised passwords and/or user IDs must be immediately changed.

13. Any unauthorized attempt to discover the password of another user or to access Bank Group information or systems using another person’s password or user ID is prohibited.

Viruses and Malicious Code

14. Contractors must use up-to-date malicious code protection and virus protection software for all systems and devices used to carry out Bank Group business.

15. Contractors are prohibited from introducing viruses or malicious code into Bank Group systems, software, or devices. This includes peer-to-peer file sharing programs.

16. Contractors are prohibited from attempting to bypass Bank Group virus protection software or other system safeguards (e.g. when downloading or transferring information).

17. Contractors must always use installed Bank Group virus protection software and other system safeguards. Contractors must scan all files and software before introducing them to Bank Group systems.

18. Contractors must not install or use non-certified software (i.e. software that is not licensed) for any purpose unless specifically granted an exception that is authorized by their Project Manager.

Information Systems and Storage

19. Personal computers, laptops, personal digital assistants (PDAs), and other devices containing Bank Group information must be secured by their users from theft and unauthorized use.

20. To ensure information security and integrity, Contractors must always completely log out from all applications, leave desktop computers in the SMS ready state, turn off

peripheral devices, and lock cabinets and other information storage containers at the end of each day.

21. All systems and software packages must be fully tested for system compatibility and the presence of malicious code and covert channels by the Information Solutions Group before use.

22. 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.

23. Contractors may not remove equipment from Bank Group facilities without management authorization.

24. Contractors may not leave unattended any device containing Bank Group information unless a password-engaged screensaver is used.

25. Contractors must always backup critical electronic files to an appropriate network drive, particularly when using portable computers or PDAs.

Incident Reporting

26. All information security incidents (e.g. malicious code, worms, viruses, unauthorized or inappropriate email/internet use) must be immediately reported to a Project Manager upon discovery.

27. Loss of 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 to ensure that its use to access the Bank Group’s network is disabled.

Telecommunications Security

28. 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.

Remote Access

29. Remote access refers to contractors using telecommunications/remote access to conduct their normal activities from a remote location.

30. All Bank Group-owned desktop, portable or mobile computing devices must employ access control and user authentication devices that have been approved by the Project Manager for access to the Bank Group's network.

31. Authentication and information on wireless medium must be encrypted end-to-end.

32. 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.

External Service Provider Requirements

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

34. The ESP must provide an overview of their information security management system including information security policies for Bank Group review prior to the engagement.

35. 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.

36. A Service Level Agreement must be part of the contract between the ESP and the Bank Group.

37. 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 Information Security Office in writing.

38. Any change in operational or security administration personnel assigned to Bank Group information systems must be communicated to the Sponsoring Business Unit and the Information Security Office in writing.

39. 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.

40. No Bank Group staff other than those authorized by the Sponsoring Business Unit should be given access to Bank Group information and systems.

41. 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.

42. The ESP must provide satisfactory responses to the Bank Group's Information Security Compliance Questionnaire before the award of a contract. The questionnaire will be provided by the Sponsoring Business Unit and approved by the Information Security Office.

ESP Communications and Operations Security

43. 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.

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

45. 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.

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

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

48. Host and network intrusion detection must be employed by the ESP where Bank Group systems are located.

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

50. 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.

51. All activity 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.

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

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

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