Experis at IBM Technical Services Security and Use Standards

This document describes the basic computer security measures that must be followed by all Supplier personnel, and others authorized by IBM management to use IBM internal computer systems. Supplier will ensure that its Personnel, Affiliates and subcontractors (“Supplier Personnel” or “you”) agree to and comply with these standards.

Section 1: Workstation Security Requirements

1.1 Security of the IBM personal workstation
You are responsible to help reduce the possibility and consequences of theft of all personal IBM computing resources and devices and the information they contain.

The following security controls must be activated on all personal workstations:

- Activate a power-on password and a hard disk password in the ThinkPad's BIOS settings.
- Activate a power-on password in your desktop workstation BIOS settings.
- Set a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 30 minutes.
- Encrypt local Lotus Notes databases (those residing on your workstation) that contain IBM Confidential information, including mail files, archives, "my attachments repository", and database replicas.

For setting power-on and hard disk drive passwords and encryption of local Lotus Notes databases refer to the NETWORK COMPUTING GUIDE Chapter 12.1 "Security Tips & Procedures for IBM Personal Computers (PCs)".

Note: You are not required to periodically change your workstation’s power-on, hard disk, and keyboard/screen lock passwords.

Note: Desktop workstations located in Controlled Access Areas or in offices, which are locked when unattended, are not required to have power-on and keyboard/screen lock passwords applied.

1.2 When Leaving Your Office or Work Area
If you work in an office that can be locked, and where local health and safety or real estate regulations allow, lock the office.

If you do not work in an office that can be locked:

- Activate the password protected keyboard/screen lock when you leave. (i.e., do not leave the workstation exposed for the 30-minute inactivity period required for the automated screen lock activation.)
- Lock up all materials that contain IBM Confidential information, or take them with you.

If the IBM ThinkPad cannot otherwise be physically secured (i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken with you), a cable lock must be used to secure the ThinkPad to a fixed object. The Kensington Master Lock is recommended.

Note: If additional security controls are required, you will be notified by the IBM manager or the location Security department.
1.3 When Traveling or Working away from Your Office or Work Area

- Keep ThinkPads in your possession if at all possible.
- When traveling by air, do not put ThinkPads in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
- ThinkPads should not be left for an extended period of time in an unoccupied vehicle. If you must leave the IBM ThinkPad in an unoccupied vehicle, then consider securing the ThinkPad to the body of the vehicle inside the trunk. Information regarding how to best secure ThinkPads in a vehicle can be obtained from the IBM location Security department.
- If you must leave the ThinkPad in a hotel, lock it in the hotel safe if one is available. If a safe is not available and you have a locking cable, use that mechanism.
- If you are traveling with IBM Confidential material recorded on portable media such as paper, diskettes, WorkPads, notebooks, etc., you must protect this media according to the same guidelines listed above for protecting your ThinkPad.

Note: If the IBM ThinkPad, or IBM Confidential information, is stolen or lost, you must report the loss to the IBM location Security organization and Supplier management.

1.4 Security of Handheld Devices

Hand held devices (WorkPads, Personal Digital Assistants, RIM BlackBerry, mobile phones with data access, etc.) require physical and logical access controls if IBM Confidential or other business sensitive data is accessed or stored by the device. The following actions are required:

- Keep hand held devices in your possession if possible.
- Activate a power on password and a password controlled time out / lock out feature on all hand held devices supporting these security features.
- Remote Synchronization via modem to move the IBM data between the device and the IBM workstation must go through an IBM authorized remote access gateway.

1.5 Computer Viruses and other Harmful Code

Install and run an IBM-approved AntiVirus program on your workstation.

If you are running the standard client for e-business (C4eb), Norton Anti-Virus is the approved program, and it should already be installed on the workstation. If you are not running a C4eb client, or if an Anti-Virus program is not installed on your workstation, refer to the IBM STANDARD SOFTWARE INSTALLER (ISSI) website to determine if an AntiVirus program is available for the IBM workstation.

Note: If an approved AntiVirus program is not available for the workstation's operating system from ISSI, you are not required to take any additional action to obtain and install an AntiVirus program.

Additional information about IBM's AntiVirus program and processes is available from IBM's VIRUS CERT website.

If you are using Norton Anti-Virus, you must also run Norton Anti-Virus LiveUpdate at least weekly to keep your Anti-Virus signature files current.

If you discover a virus, complete the on-line form available on IBM's VIRUS CERT website.

Use Lotus Notes Execution Control Lists (ECLs) to define trusted signers of executable content and to assign appropriate default levels of access.

If you are running the standard client for e-business (C4eb), appropriate ECL settings have been set. If you are not running a C4eb client, or if you have special ECL needs, refer to the NETWORK COMPUTING GUIDE Chapter 5.12 "Lotus Notes Workstation Execution Control List - ECL" for complete description and ECL settings.
1.6 **Security Firewalls**

Install and run an IBM-approved personal firewall program on your workstation if you directly connect the workstation to any Customer network, or to the Internet via DSL or Cable Modem, or to any wireless network.

Refer to the IBM STANDARD SOFTWARE INSTALLER (ISSI) website to determine if an approved personal firewall program is available for your workstation's operating system.

Additional information about approved firewall programs and processes is available from the Symantec Desktop Firewall/System Security Services section of IBM's VIRUS CERT website.

*Note: If an approved personal firewall program is not available for your IBM workstation's operating system from ISSI or from the virus CERT website, you are not required to take any additional action to obtain and install a personal firewall.*

1.7 **File sharing**

You may only allow other users to access or store files on an IBM network-connected workstation under the following conditions:

- The software that allows other users to access your files must be provided by IBM (this is to ensure that it has been adequately checked for security holes and legal and licensing restrictions).

*Note: The use of Internet-based peer-to-peer file sharing services, such as Napster and KaZaA, on IBM workstations is prohibited unless explicitly approved by the IBM Business Transformation / CIO security staff.*

- You must not allow anonymous FTP, TFTP, unauthenticated HTTP, or other unauthenticated access to areas of your hard disk that are also used for other purposes. For instance, you may not "share out" your entire hard drive with anonymous access.

- You must not allow any form of unauthenticated access to data or programs that are classified IBM Confidential, or to areas of your hard disk that may contain such data or programs.

- If it is necessary to allow access to areas of your hard disk that are also used for other purposes (for instance, to allow remote maintenance or update of components of the operating system), or to IBM Confidential materials, you must select either userid access control or password access control when defining the share options and the access must be granted only to the limited list of people with a need for that access (not, for instance, to anyone who authenticates with an IBM intranet password).

For advice on how to configure your system to share files securely, refer to the NETWORK COMPUTING GUIDE Chapter 12.8 "Sharing Access to Network Resources", or contact your local Provider of Service.

1.8 **Contractors Providing Unique Services**

For certain work being performed under the SOW, Supplier may be required to provide their personnel with the appropriate hardware and software. In cases where LAN connectivity to IBM’s network is required, Supplier must ensure:

- All software on the Supplier provided equipment must be compatible with the IBM platform.

*Note: Software provided by IBM (with appropriate license agreements in place) will be tracked by IBM management and upgraded at the same intervals as IBM workstations to ensure compatibility.*

- An IBM-approved version of Anti-Virus software must be installed on all workstations.

- While connected to the IBM LAN, Supplier personnel are prohibited from connecting to other networks/resources, except as provided by IBM management.

- All Supplier personnel must adhere to IBM’s policies regarding the use of proprietary information and ITCS300 (Computer Security and Use Guidelines) regarding the appropriate use of equipment on IBM’s network.

- All IBM data including access information and passwords must be deleted from the system when there is no longer a legitimate need and authorization for access.
Additionally,
• Upon request from IBM, Supplier will retrieve IBM data from specified workstations and inspect designated machines. Supplier will take necessary actions to protect IBM proprietary information.
• IBM is released of all liability in the event of loss/damage to the contractor’s equipment and/or information.

**Section 2: General Security & Use Requirements**

**2.1 IBM Management Approved Use of Computer Services**
Computer systems provided by IBM to you for use in your work for IBM must only be used for conducting IBM's business or for purposes authorized by IBM management. All electronic documents created, stored, or communicated using IBM's computers are the property of, or under the custody of, IBM. IBM may access documents or communications stored on its property or in its systems when appropriate, such as when warranted by business need or legal requirements. IBM reserves the right to monitor its systems for reasons including accounting purposes, to ensure proper use, and to detect security violations. You should not expect that your communications using IBM’s systems are private. Use is subject to audit at any time by IBM management.

**2.1.1 Personal Use of Computing Equipment**
Personal use of IBM computing equipment may only be approved by IBM management if use is clearly insignificant compared to your business use. For example, personal use will not be approved if it:

- Interferes or competes with IBM business
- Interferes with your job or the job of other IBM employees or Customers
- Involves any incremental cost to IBM
- Involves commercial solicitation
- Provides information about, or lists of, IBM employees to others
- Involves commercial or personal distribution lists.

Access to the Internet from the ibm.com business address designation and the use of IBM's e-mail systems are intended to be for IBM business related activity. However, incidental and infrequent personal use of IBM's e-mail systems and access to the Internet for personal use during or outside your normal work hours are allowed without IBM management approval provided none of the above prohibitions are violated.

Questions concerning personal use of IBM computing resources and Internet services should be discussed with the IBM manager.

**2.1.2 Chain letters, Hoaxes and Virus Warnings**
Chain letters and hoaxes come in many versions, for example offering a free trip or a large amount of money, warning about a computer virus, or relating to a sympathetic cause. These letters often request that you send them on to other people.

Using IBM computer systems to send or reply to chain letters, hoaxes, or virus warnings is prohibited.

If you receive an e-mail chain letter or virus warning, don't forward it!

If you receive an e-mail notice about a supposed virus or harmful code threat, check IBM's VIRUS CERT website to see official information on real and hoax alerts.
2.1.3 **Offensive and Inappropriate Material**
You are not to access or distribute any material that could be considered inappropriate, offensive or disrespectful to others. While it is impossible to list every form of such material, some clear examples include:

- Materials that contain sexually explicit images or descriptions
- Materials that advocate illegal activity
- Materials that advocate intolerance for others

You should discuss questions concerning inappropriate or offensive material with an IBM manager or Supplier management.

2.1.4 **Web Cameras**
The use of web cameras or similar technology is prohibited without IBM management approval.

2.2 **Legal Considerations**

2.2.1 **Software Licenses**
You must have a valid license for all licensed software that you personally obtain and install on an IBM computer. Your Provider(s) of Service are responsible for licenses of software they obtain and install for you.

Never copy or duplicate licensed software, except as explicitly allowed in the license terms and conditions.

2.2.2 **Copyright and Intellectual Property**
Most information and software (programs, audio, video, data files, etc.) that is available in the public domain (including on the Internet) is subject to copyright or other intellectual property right protection. When obtaining material for use inside IBM:

- Do not obtain software from such sources for use within IBM unless express permission to do so is stated by the material owner.
- You must read and understand any software copyright restrictions. If you think that IBM will not be able to comply with any part of the terms, do not download or use the material.
- Ensure that you comply with any expressed requirements or limitations attached to the use of such software (for example: not to be used for commercial purposes; can not charge others for use or distribution; subject to a copyright or attribution notice being affixed to each copy; must distribute source code; etc.).
- If you are unsure about the meaning of the restrictive language or have questions about it, you should contact an IBM attorney to review it before downloading or using the material.
- You must obtain assistance and approval from IBM Legal or Intellectual Property Law counsel before incorporating any public domain material into a product or material IBM intends to distribute externally.

2.2.3 **Privacy (Data Protection) Legislation**
The collection, storage, use, disclosure, and the transfer of personal information to other countries may be subject to privacy legislation and restrictions. This includes personal information about IBM employees and Customers as well as information collected on other individuals as part of normal business responsibilities.

Many countries also now have laws with specific restrictions regarding "Who, What, Why and Where" a Customer, or potential customer (commonly referred to as a Customer contact, or data subject), may be contacted. These restrictions are particularly relevant on the Internet. In general, you are not to initiate any communication with a Customer contact, without prior approval from that contact.

If you have questions regarding the protection of personal information or regarding contacting Customers outside your country, you should seek advice from the IBM manager and/or local legal department.
Section 13 of the SOW provides the minimum framework that all IBM supplier personnel must follow in every country. If more restrictive local legislation exists, then you must ensure the local laws are followed in addition to the SOW requirements.

2.2.4 Protecting Another Company's Classified Information

If you receive another company's classified data, you must comply with that company's instructions for protecting the data. Any questions concerning protection of the information should be discussed with the IBM manager or IBM's local legal counsel.

2.2.5 Releasing IBM Information into the Public Domain

Seek advice from the IBM manager or IBM Intellectual Property Law counsel before uploading any IBM software to the Internet. You must ensure that any IBM copyright documents clearly indicate IBM as holder of the copyright.

2.3 Protecting IBM Information

2.3.1 Passwords

The password associated with a computer access userid is the primary key to verifying your identity, and subsequently allowing you access to the computer and to IBM information. For your own protection, and for the protection of IBM's resources, you must keep your identity verification password secret and not share it with anyone else.

*Note: The power-on and hard disk passwords you use to help protect against unauthorized access to your workstation are not identity verification passwords. It is not a violation of security policy for you to notify your manager and the IBM manager of these passwords, as per the instructions in the Network Computing Guide.*

The following guidelines are designed to help you select passwords that are not trivial or predictable, and are resistant to compromise by computer "hackers". Identity verification passwords must:

- Be at least 6 positions in length
- Contain at least one alphabetic and one non-alphabetic character
- Contain an alphabetic or other non-numeric character in the first and last position
- Contain no more than three identical consecutive characters in any position from the previous password
- Contain no more than two identical consecutive characters
- Not contain your userid as part of the password

IBM internal business systems and applications containing IBM Confidential information require you to change your password at least once every six months. In cases where the system or application does not use technical control measures to force you to change your password, it is your responsibility to comply with the password change requirement. When changing your password, you must select a new password, i.e., do not change the password to one that you used in the past.

*Note: If you access computer systems that are not under IBM control, do not select the same password on external systems that you selected for use on IBM internal systems.*

2.3.2 Lotus Notes Calendars

You must ensure that your Lotus Notes Calendar can only be viewed by authorized individuals such as your department/team members and/or your administrative assistants.

For instructions on how to set your Lotus Notes calendar to only allow authorized individuals to view your calendar, refer to the NETWORK COMPUTING GUIDE Chapter 12.1 "Security Tips & Procedures for IBM Personal Computers (PCs)".
2.3.3 Protecting IBM Confidential Information
The primary requirement for protecting IBM Confidential information is that it must be protected from access or viewing except by people who have a business need to know the information.

IBM requires the encryption of IBM Confidential information when it is sent over the Internet, public networks, or wireless devices. Refer to the NETWORK COMPUTING GUIDE Chapter 6.17 "Encrypting Mail Between Notes and Non-Notes Users" for additional information about encryption tools.

When you store IBM Confidential information on computer systems (e.g. group web sites, Lotus Notes databases, or other shared data repositories), you must use software security controls to manage and limit access to the information. Security controls must never be set to allow unrestricted access (e.g., World-readable, “public”) to IBM Confidential information. If you do not understand how to correctly set or use the security controls, you should ask for advice or assistance from your Provider of Service.

When you store IBM Confidential information on removable computer media, such as diskettes, tapes, compact disks (CDs), handheld device storage, etc., you must protect the information against theft and unauthorized access. Label the media IBM Confidential and keep them in a locked area or storage device when they are not in use. Never leave them exposed in unattended areas.

Do not store or process IBM Confidential information on systems that are not controlled by you or IBM.

Do not enter IBM Confidential information on Internet web sites that offer translation services, e.g. world.altavista.com.

When printing IBM Confidential information you must protect the information against theft and unauthorized viewing. (The term "printer" includes printers, plotters, and any other device used to create hard copy output.) IBM Confidential information may only be printed: in a controlled access area, with access based on 'need to know', or; in an attended IBM printer facility, where the output is given only to its owner, or; on a printer with capture/release facility that you control, or; on a printer that you are personally attending, or; if Printing Systems Manager (PSM), or an equivalent function, is available in the location where you are working, use it to control printing.

For additional information, refer to the NETWORK COMPUTING GUIDE Chapter 9.4 "Managing Your Print Jobs With PSM (Including Canceling, Holding, Delaying)". If none of these options are available at your location, you may use a printer located within an open area in IBM internal office space, but you must pick up your IBM Confidential printout material within 30 minutes.

2.3.4 Using Telephones, Facsimile (FAX) and Pagers
The use of telephones outside IBM to discuss IBM Confidential information is sometimes necessary, but it can create security exposures.

- Take care that you are not overheard when discussing confidential matters.
- Avoid use of any wireless or cellular phones when discussing IBM Confidential information.
- Avoid leaving IBM Confidential messages on non-IBM voicemail systems. If you routinely use a non-IBM voicemail system for IBM business purposes, advise callers in your "greeting" not to leave IBM Confidential messages.
- If sending IBM Confidential documents via FAX, verify the phone number of the destination FAX. Contact the recipient to ensure protection of the fax, either by having it picked up quickly or by ensuring that the fax output is in a secure area.
- Do not use Internet FAX services to send or receive IBM Confidential information.
- Do not use third party FAX services to send or receive IBM Confidential information.
- Do not send IBM Confidential documents via wireless FAX devices.
- Do not send teleconference call-in numbers and passcodes to a pager, if IBM Confidential information will be discussed during the conference.
2.3.5 **Using Teleconferencing Systems**
When chairing an IBM Confidential teleconference, confirm that all participants are authorized to participate, before starting any discussion.

2.4 **IBM Internal Networks**
When connected to and using IBM internal networks, including Local Area Networks (LANs):

- Do not misrepresent yourself (i.e., masquerade) as someone else on the network.
- Do not monitor network traffic (i.e., use a “sniffer” or similar device) without first obtaining explicit management approval and permission from the network administrator.
- Do not run security testing tools/programs against any Intranet system or server, other than those that you directly control, without first obtaining explicit management approval.
- Do not add any network device that extends the IBM infrastructure (e.g., devices or devices functioning as: Switches, Bridges, Routers, Hubs, modems, wireless access points, etc) for any reason without first obtaining permission from the network administrator.

2.5 **Computer Conferencing**
IBM internal computer conferencing (Newsgroups, Forums, Discussion Databases) provide company-wide databases for sharing information and discussing ideas about a wide range of business related topics, as approved by the conference owners.

Information and discussions on IBM internal conferences must meet the following criteria:

- If the conference is set up to allow open participation within IBM, or to allow participation by IBM Customers or other external parties, IBM Confidential information must not be included or discussed.
- Nontechnical information and comments which are more appropriate for an official IBM communications channel (e.g., speaking to one's manager, the Speak-Up Program, the Open Door Program, etc.) must not be included.
- Participants are to avoid giving legal opinions or medical advice.
- Secure computer conferencing services must be used when IBM Confidential, personal or sensitive information is discussed. (IBM's E-MEETINGS service provides secure computer conferencing services.).

2.6 **External Connections and Remote Access**
Connecting IBM systems and networks to non-IBM systems and networks, including the Internet, through modems or direct-line attachments, can present a serious risk to IBM.

If you need to connect to non-IBM systems or networks from inside IBM (e.g., to the Internet, to a business partner's system, etc.), you must use one of the approved IBM IES gateways. Check with your Provider of Service to determine what IES services are available for your use.

If you need to connect to IBM systems and networks from outside IBM premises, you must be registered to use one of the approved remote access services. Check with your Provider of Service to determine how to register to use one of these services.

2.7 **The Internet**

2.7.1 **Conduct**
When accessing the Internet from ibm.com or other IBM designated addresses:

- Never masquerade as someone else.
- Use only services you have authorization to access.
- Do not run security testing tools/programs against any Internet system or server.
When using electronic mail to communicate with people on the Internet:

- Do not automatically forward IBM internal mail to an Internet site.
- When sending or forwarding e-mail to the Internet, do not include the names or user ids of other IBMers unless required.
- Do not use auto-reply functions to respond to your Internet mail. If you use auto-reply functions such as the Lotus Notes Out of Office message option for your normal IBM internal mail when you are away, be sure to select the option that excludes sending the notices to Internet users.
- Do not use non-IBM e-mail, e.g. Yahoo, AOL, Hotmail, etc. to exchange IBM information.

2.7.2 Receiving Unsolicited e-mail
If you are holding an Internet e-mail address, you may be recipients of unsolicited non-business e-mail (sometimes referred to as Spam or junkmail). This situation is very similar to receiving unsolicited telephone calls or unsolicited postal mail.

If you receive unsolicited e-mail, refer to the ABOUT UNSOLICITED E-MAIL, OR SPAM website article for current advice regarding how to handle such e-mail.

2.7.3 Privacy
Information known as "cookies" may be placed as a file on your system by web sites (including IBM web sites). In some instances, other web sites can browse your cookie file and find personal information. Cookies may be helpful but be aware that they persist until you manually erase them. You should erase unwanted cookies regularly. Cookie settings may be changed in your browser preferences.

For security guidance related to your browser, you should refer to the NETWORK COMPUTING GUIDE Chapter 13.1.2 or 13.2.2 "Cookies".

Section 3: Security Incident Reporting

If you suspect a security incident is in progress or has occurred, it is important for you to act promptly by contacting the IBM location Security department.

You are not to attempt to investigate or take action against the offender unless directed to do so by Security personnel. The Security staff is qualified and trained to properly contain exposures, mitigate potential impact to IBM, and conduct investigations, up to and including gathering evidence for possible legal action.

If you have security questions, discuss them with the IBM manager, local security, or visit the IBM CORPORATE SECURITY WEB SITE.

Section 4: Geographic Considerations

IBM country, or geographic Human Resources and Legal functions, will determine ITCS300 deviations necessitated by local laws or industrial relations agreements, and will provide appropriate guidance to the IBM managers/employees in countries affected by the deviations. Supplier will inquire when work is not being performed in the US as to any deviations which apply.

Section 5: Acknowledgement

My signature certifies that I have received, read and acknowledge the Experis at IBM Technical Services Security and Use Standards, and that I am responsible for abiding by these guidelines, which apply during the course of my assignment at IBM.