IBM Data Security and Privacy Principles for IBM Systems Unit

Version: November 20, 2017
Status: Approved
Revalidation Due: November 20, 2018

Disclaimer:
This document describes the IBM practice regarding data security with respect to customer data processed and stored by IBM in the provision of hardware support for products offered through The Offerings (see chapter 1, 'Introduction') and the purchase of hardware. While remaining consistent with the general guidance herein, each such offering or purchase may differ in the details of their security infrastructure and procedures.
This document will explain our data security practice for such offerings and purchases; however, IBM MAKES NO WARRANTY, EXPRESS OR IMPLIED, THAT THESE SECURITY PRACTICES ARE SUFFICIENT TO ENSURE THE SECURITY OF CUSTOMER DATA. Customers are directed, in the case of IBM SaaS offerings, to the Data Security and Privacy Principles for IBM Cloud Services at http://www.ibm.com/cloud/data-security. In the case of product support, customers are also directed to the online descriptions for support procedures and tools as listed in Chapter 11, 'Service and Support.' IBM products and services, including those from IBM Subsidiaries or acquired companies, and any offering that is not acquired through The Offerings are excluded from this practice.

Contents

Preface

Many internal processes and tools referenced in this document are proprietary and/or confidential and are only described here in part, as they relate to protecting customer-owned data and are not described in sufficient detail to enable those so-inclined to compromise them.

1. Introduction

This document, called **“Data Security and Privacy Principles (DSP)”** for short, describes generally the set of principles, processes, controls, and tools that IBM uses with respect to customer-owned data provided by a customer or otherwise collected by IBM in the provision of certain hardware support or hardware related offerings provided by IBM (called “Customer Data” in the rest of this document). This document only applies to hardware support, associated hardware offerings and services acquired by customers under IBM’s Partner World, PassPort Advantage, Passport Advantage Express, Flexible Contract, Monthly Usage or License Charge, One-Time Charge, and Software/Hardware Maintenance contracts (The Offerings) or Business Partner Agreements. Customer Data is data that originates with a customer and provided to IBM to access, store or manage as part of the offerings referred to above. Customer Data can be managed by IBM or come into IBM’s possession as part of The Offerings in several ways: (i) customer use of The Offerings, (ii) customers may send data for use in software or hardware support (e.g., debugging data such as contained in storage dumps), and (iii) customers may return equipment for upgrade, exchange, or repair, and the equipment may contain residual Customer Data. In addition, the exact implementations of certain processes, tools, or configurations may be highly security sensitive and will not be disclosed here. Missing details may include, for example, low level security settings for firewall rules, which are known only to the security teams responsible for implementing them and the audit teams responsible for verifying them.

Scope Definition

The DSP is restricted in scope to the description of the handling and protection of Customer Data by IBM in its provision of product support, services and offerings. Special compliance measures required by specific laws or regulations applicable to certain customers are not in the scope of this DSP.

This DSP focuses on IBM’s business infrastructure and operations, and only on production systems (test, demonstration, and other systems are out of scope).

Customer Data is kept on production systems (servers and workstations used for production business purposes). However, if required, to reproduce an error using a configuration similar to a customer’s, Customer Data may be put on non-production test machines on isolated networks. Test machines are isolated to networks that are not reachable from outside IBM and are only reachable by production systems inside IBM through restrictive flow devices. For more on the layered network security approach IBM uses to isolate networks and create security zones, please see "Network Security."

IBM and Security

IBM has a long history of focus on security issues from a hardware and software technology point of view, but also from a business practice point of view. The IBM security management system is comprised of corporate requirements for the end to end management of security. The IBM security management system provides an overall framework and set of requirements related to: Risk Analysis, Physical Security, Emergency Planning, Investigations, Information Protection, Education, and more. That IBM security manual and all of the other sources used for this DSP are derived from IBM Corporate Instructions (IBM internal business controls described later) and so are authoritative business controls. IBM's security practices take a broad range of potential risks to data security into consideration, including technological, human, and natural. Threats come from outside an organization and can come from within it as well.

One of the main Corporate Instructions for information technology security sets out guidelines and requirements for IT security, including the protection of data, including Customer Data. Some of those guidelines and requirements (and others) are summarized in this DSP.

2. General Data Security Principles

IBM highly prioritizes Customer Data security. The security of facilities, people, and data are all ingrained into the business controls that guide the organization. This short section describes some of the underlying security principles that inform IBM security policies and procedures.

Compartmentalization

Compartmentalization is the act of limiting access, whether physical or logical, to those personnel who genuinely need it to perform their jobs. IBM limits authorized physical access to data centers, for example, to personnel with a business reason to be there. (In fact the vast majority of IBM employees have no physical access to any data center.) IBM also limits authorized logical access to applications and databases, for example, to personnel whose job function requires it.
Compartmentalization is a technique that helps control risks associated with accidental or intentional human behavior.

Least Privilege

The principle of least privilege is applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. This principle is applied both physically and logically. Organizations are required to assess and determine what level of privilege is required based on business purpose/need.

As an example, physical access to Controlled Access Spaces/systems is granted to specific areas based on need (e.g. an administrator may require access to a data center, but this does not qualify that administrator for access to all data centers. Similarly, in the case of logical access, a database administrator would only be allowed access to the specific data and functions to complete tasks that are aligned with the defined business need.

Separation of Duties

Separation of Duties is the principle of checks and balances. For example, an IBM person who administers a particular database should not be the same person who audits the security procedures for that database. Separate people or groups exist to check on each other. This limits the potential of an abuse of authorized privileges and the risk with associated activities. IBM practices extensive separation of duties. For example, the software area business controls team is independent from any of the organizations they audit.

Defense in Depth

Defense in Depth refers to the practice of creating multiple layers of security. Instead of a simple physical or logical block, beyond which there is free rein, multiple blocks are placed in succession, like layers of an onion. The layered approach to security helps prevent many types of attacks from being carried out. A failed block in one place is essentially backed up by other blocks. An example of physical defense in depth is requiring badge access to a building, then also badge access to a data center and then also maintaining separate access control to server cages within the data center. This creates three layers of security. Site access adds a fourth layer and there can be more.

Logical defense in depth is analogous. For example, multiple, onion-like layers of firewall protection are employed. This layering approached is described in more detail later in this document.

Continuous Improvement by Design

Business controls and security management systems are designed to be improved as time goes on and conditions change. They have expirations or re-approval dates. For example, this DSP is revalidated at least annually. During revalidation, the DSP is examined in light of any changes that have occurred and adjusted accordingly. The DSP itself requires that it be reexamined and improved (see title page for current DSP revalidation status).

IT Risk Management

Risk assessment and risk management are fundamental foundations of data security.
For IBM, there is an IT Risk Management Steering Committee headed by the IBM CIO. Members of the committee are security professionals, executives, and people who create internal IT standards for management approval. The function of this committee is to continually examine IT risks across a broad spectrum of potential threats. The output of this committee is used to improve IBM’s IT risk posture. Our internal business controls staff periodically audits for compliance (i.e., integrated into business controls).

3. Physical Security

Facilities and Access Control

IBM employs access control mechanisms to limit access to system assets and infrastructure components. Keys, cipher locks, electronic controlled access systems, guarded entrances, and in some cases biometric controls are all examples of physical access control employed by IBM.

Controlled Access Space(s) (CAS) are categorized according to a set of CIO defined criteria to identify and protect facilities, contents, and people.

Personnel are given authorized physical access to CAS only with business justification. Depending on that person's job responsibilities, access may be restricted to only a portion of the facility.

Access to CAS is logged and the logs reviewed either by automated tools or manually according to guidelines. The guidelines also specify timing requirements for log reviews and for site reviews of physical security procedures. Documentation including security review evidence is required to be kept according to IBM Worldwide Records Management policies.

Every CAS has an identified owner responsible for the implementation of proper policies and controls related to the CAS. CAS are required to be locked even when occupied. External windows are generally not permitted, especially for ground floors, with limited exceptions documented.

Site specific security procedures applicable to a CAS are required to be documented and tested.
For instances where a CAS is contained in a non-IBM owned facility, security requirements are detailed by contract and the owner of that facility agrees to abide by those requirements.

Media and Physical Disposal of Media

Only approved carriers are used to transfer electronic media that may contain unencrypted data. Server media used for backup, records retention, or disaster recovery is required to be physically protected against unauthorized use, theft, and damage.

Server storage Media Custodians handling Customer Data are responsible for accurate media inventory and for reporting any discrepancies according to and using IBM's Security Incident Handling Process (SIHP). In keeping with the separation of duties security principle, at least one person not involved in the media operation must perform the inventory (the Storage Media Custodian may participate, but is not permitted to be solely responsible for performing the inventory).

Physical media received from customers is handled separately from IBM data, but is also inventoried and handled in a controlled manner. Records are kept concerning its lifecycle from being shipped to IBM to its being disposed of, either returned or destroyed.
Media, storage devices, and computing devices being returned to an IBM asset center must be "wiped" to render the data unreadable before shipment.

4. Logical Security

Logical security consists primarily of technical measures that are implemented at the system, network and end user level.

A few common logical security measures apply to networking infrastructure, servers, and workstations. These measures include:

- Access controls (more details in individual sections below)
- Technical measures to address propagation or execution of unapproved code (e.g., viruses and other malware). Updates are done automatically wherever possible (such as workstation anti-virus updates) or periodically on a prescribed, prioritized schedule.
- Periodic vulnerability scans and/or penetration testing.
- Policies are applied dictating security advisory actions (such as patch management within x days for high severity problems, y for next highest, and so on, based on category of device). Patch management is required to be done on a timely basis, based on a classification scheme of systems and the severity level of the patch, and sometimes even based on the operating system type or release.
- Technical controls to prevent denial of service attacks (primarily applicable to network infrastructure and servers).
- Creation and capture, if the device is capable, of activity logging records (network infrastructure and servers) that can be accessed for audit and by "suspicious activity" monitoring tools. The length of time such log records must be kept is determined by IBM Worldwide Records Management (WRM), which categorizes and details retention requirements. A list of suspicious activities to be monitored is maintained by CIO.
- Requirement to follow specific security measures for remote access to IBM internal systems from outside the logical firewall, including a mandatory VPN client. All such access is encrypted. (Applicable to workstation and mobile devices.)
- Requirement that devices are to be cataloged in a database used for control and audit purposes.
- Requirement to use static IP addresses (DHCP/DDNS are generally not permitted, except in some approved and documented cases for servers, and for workstations generally). All static IP addresses are recorded in a secure database.
- Requirement to present at each log in to IBM systems that they are for business use only, and where permitted by law, this includes notice that any system can be audited for appropriate business use at any time.
- Requirement to use specific CIO guidelines to build operating system images (workstations or servers).

- Requirement to ensure that systems maintain a secure configuration (e.g. Password Strength). All systems and services must pass a security health check to verify that system parameters are set in accordance with a Platform Technical Specification (low level CIO defined specifications for every type of infrastructure device, server, and workstation / mobile device) prior to initial service activation and periodically according to a mandated check schedule. These health checks are part of a broader independent audit process detailed later.

Where permitted by law, Security Technical Testing (STT) is performed by teams of individuals with highly specialized skills who are allowed to use their skills, tools, and techniques to discover potential exposures that would not normally be found during routine testing. This is sometimes referred to as "white hat testing" or "ethical hacking." There are established resources within IBM to assist individuals performing STT, including process overview documentation.

Technical Specifications for Servers, Middleware, and Applications

IBM maintains detailed technical specifications for security that are specific to each operating system, each middleware product, and deployed applications. Sometimes these technical specifications are even by specific release, as operating system releases, for example, can add new types of configuration settings or vulnerabilities. The detailed low-level specifications are maintained by the CIO. Compliance with the technical specifications is required for all production servers, middleware, and applications, including those handling Customer Data. Compliance is independently audited by third parties.

Information Classification

IBM classifies information to identify its required protection characteristics. Certain types of data require different protection characteristics. For example, any personally identifiable information (PII) is subject to regulations within the European Union (EU) member states and many other countries and US states (such as Massachusetts). This type of data requires extra controls that are mandated by the regulatory authorities. Included in this scope is the EU General Data Protection Regulation (GDPR). IBM's commitment to GDPR readiness can be found at:
http://ibm.com/gdpr

Special handling for regulatory compliance is beyond the scope of this DSP.

Role Based Access

Access to information is both individual and role based. Role based access is granted to individuals when the individuals role aligns to the stated business need for access. As an example, server administrators would not be granted administrator access to the databases that reside on their servers.

Identification and Authentication

IBM production systems require authentication for access. This includes network devices, servers, workstations, and some types of applications. Some systems require user ID and password or digital certificate while others require multi-factor authentication ("something you know plus something you are or have," such as password plus biometric scan, or password plus security key fob). Multi-factor authentication is required for any system available over a public network or for any privileged user with system authority.

Each employee has a unique user ID and password (at a minimum) for a particular system or intranet. User IDs and passwords are only created based on job function need (the job role) of the individual. User IDs and passwords are not generated unless a business need is evidenced and documented.

In certain limited circumstances, use of shared IDs is allowed, but each individual authorized to use a shared ID is identified and must meet executive approval prior to use.

Password rules apply. Most passwords are required to be changed at least every 90 days. Passwords are required to be of a certain length and contain certain combinations of letters, cases, numbers, and other special characters. In addition, incorrect password attempt rules are in force, such as disallowing access after a certain number of incorrect attempts. Automated tools (where possible) remind users to change passwords and enforce the password rules.

Non-expiring passwords are generally not allowed, with very limited exceptions (e.g., laptop hard drive passwords are exceptions, but these passwords only come into play if a drive is removed and reconnected to a “foreign” controller).
Digital certificates used for identification must be from an IBM CIO-approved certificate authority.

Network Security

Network security involves both physical and logical security measures. From a logical security perspective, IBM partitions its IT infrastructure into security zones with flow control devices, such as firewalls and routers, governing the allowable flows between security zones. This enables IBM to deploy an architecture conforming to the Defense in Depth security principle.

Any system connecting to an untrusted network, such as the Internet, is highly restricted. Connections from these highly restricted systems to any other production systems in IBM are tightly controlled. Firewalls are specified at several levels in the network architecture. Required firewall rule sets are maintained.

Physical security restrictions exist as to physical placement of network infrastructure devices inside CA’s. Additionally, routers, switches, wired and wireless access points are access controlled, as are servers and workstations. No unsecured wireless access points are permitted (with limited exceptions for non-secured guest access to the Internet). Access by authorized personnel is limited to those whose job role requires access. General users are not allowed access to network infrastructure devices.

Wireless access points are secured, but because they have to be where the users are do not always require placement in a CAS. However, detailed placement rules still apply, such as being at least a certain number of feet above ground level if not in a locked room.

Dial access to network devices is generally not allowed. “Business use only” notifications are presented to users logging in to IBM production systems, including networking devices.

Technical controls to restrict the propagation or execution of unapproved code (e.g., viruses or other malware) are required for any infrastructure device where possible.
Many controls or measures are common to several types of equipment and are discussed in the beginning of this chapter.

Server Security

Logical and physical controls apply to production server systems. Many technical controls are required for server systems, based on server use categorizations.

Server access is based on need. As elsewhere, server authorization rules follow the Principle of Least Authority, where the lowest level of authority consistent with the business need is granted. In particular, general users are not granted “super user” or equivalent privileges on production servers.

Server administrators or anyone having administrative access privileges are subject to more security requirements than general users. For example, they are not allowed to use personally-owned laptops or devices to perform any IBM administrative or elevated privilege tasks.

The IBM CIO maintains a set of hypervisor security rules and extensive low-level Technical Specifications for security settings by server OS.

Many controls or measures are common to several types of equipment and are discussed in the beginning of this chapter.

Database Security

Databases, like servers in general, have physical and logical control requirements. Databases are required to have several levels of access controls, which can also vary by the sensitivity of the data kept within them.

Highly sensitive or regulated data is generally prohibited in IBM production servers. Under special circumstances, such data can be kept under special controls, but this is outside the scope of the DSP. Database administrators, as with other elevated privilege users, are subject to more security requirements than general users.

The IBM CIO maintains extensive low-level Technical Specifications for security settings for database middleware.

Workstation and Portable Device Security

IBM employees are required to follow specific rules concerning workstations potentially used to access Customer Data. Workstations:

- Must have up to date anti-virus protection proscribed by CIO (specific anti-virus software is mandated). Virus scans are required and automatically scheduled.
- Must have log on password protection enabled
- Must have keyboard / screen lock timeout set to 30 minutes or less (in some cases 15 minutes)
- Must use the encryption option for any Lotus Notes databases that could contain sensitive information
- If the device supports a hard drive password it must be enabled, unless full disk encryption is used. However, many IBM’ers are required to have full disk encryption.
- Must be automatically kept up-to-date with security patches
- Must not contain unapproved or inappropriate software or data
- Can only use pre-approved open source software. The approval process is intended to insure that only tested and safe software is used and IBM complies with applicable terms of use.
- Must have special monitoring software programs installed that can verify compliance with security requirements and help IBM to manage end use devices (for example Tivoli End Point Manager)
- Must have specific, CIO approved Virtual Private Network (VPN) software installed to remotely access the IBM intranet. Such access is encrypted to CIO-specified strength.
- Must have an IBM-approved client firewall installed and operating
- Must not use Internet peer-to-peer file sharing applications, unless approved by CIO
- Must not allow any form of unauthenticated or unapproved access
- Must have a registered MAC address
- Obtain approved versions of IBM required software from an internal software distribution system (called ISSI, IBM Standard Software Installer)

Certain types of workstations are not permitted to be used for privileged operations. Privileged operations include administration of servers, networking infrastructure, applications, or databases for production systems.

For some types of users, portable storage media (such as a USB thumb drive) are not permitted to be used unless purchased through IBM Procurement. Only certain types of portable media with security features are allowed for these users.

In some instances, IBM employees may use workstations or laptops provided by a client. In these cases, IBM workstation rules are to be followed, unless the client requires even more stringent security rules, in which case those rules are to be followed. Portable storage media are not to be attached to any client provided asset, unless the portable media is purchased through IBM Procurement (guaranteeing the device supports required security features).

Use of personally-owned assets, such as laptops, is restricted to certain classes of users. In addition, when using a personally-owned asset, all of the same security rules are required to be followed, just as if the asset was IBM-owned.

In some cases, cable locks are required on assets.

Portable devices such as laptops are not to be left unattended in a car for an extended period (even if locked), or placed in checked baggage.

Portable devices such as smart phones used for business purposes also require controls and registration. Certain devices are supported, while others are not. Devices are required to have a power on and timeout password lock out feature. They must be configured to prevent access in the event of 10 consecutive failed access attempts. If they can be configured to remotely wipe data, that feature must be turned on. They must have anti-virus protection configured if possible. Employees are advised that synchronization should not be done over wireless, unless the wireless network is trusted (such as a secure home network). Bluetooth should be configured so that the device is not discoverable. Smartphone access to the IBM network is generally limited to email/calendar/contacts and this data is generally encrypted on the device (either natively or through Lotus Traveler).
The owner of any device being returned to an IBM asset center must “wipe” all data to render it un-readable.

Application Security

Many applications require authentication and authorization, similar to but distinct from operating system log on.

For some internal applications (those only accessible from IBM's internal network or using VPN and not highly sensitive in nature), a single sign on capability exists by logging in "to the IBM intranet." IBM intranet access alone does not allow access to all systems or applications, but allows many common non-critical applications to be accessed.

Application administrators are subject to more security requirements than general users, due to their enhanced authority level.

As previously mentioned, extensive low-level Technical Specifications for security settings for applications are maintained by CIO.

Intrusion Prevention, Detection, and Vulnerability Scanning

Intrusion prevention is deployed in various manners throughout the IBM infrastructure. Anti-malware software controls are required at several levels (several levels in the network architecture, server, and workstation). Firewalls are specified at several levels within the network infrastructure as well as for servers and workstations.

Detecting suspicious activity is also required. Many activities and accesses are monitored and logged to support suspicious activity detection. Users with elevated privileges (beyond general users) are monitored to a higher degree. A list of required security log events is maintained by CIO.

Vulnerability scanning is performed according to a schedule related to the type of system being scanned. Additional ad hoc scanning is allowed. Internet facing systems found to have a vulnerable condition are removed from service unless they can be corrected with specified time limits.
Approved scanning tools are available for system administrators and security professionals to download from the internal Security, Asset, and Risk Management (SARM) web site. Required vulnerability scan profiles are also kept there.

5. Secure Engineering

The IBM Secure Engineering Framework reflects best practice from across the company and directs development teams to give proper attention to security during the development lifecycle.
Secure Engineering practices include: project planning, security awareness education, risk assessment & threat modeling, security requirements, secure coding, source code scanning & dynamic security testing, security documentation and a product security incident response process. These practices are intended to help enhance product security, protect IBM intellectual property, and support the terms of warranty of IBM products.

For more about IBM product security, see:
http://www.ibm.com/security/secure-engineering/
http://www.ibm.com/security/secure-engineering/process.html 15

Security Incident Handling Process
IBM has a process for handling security related events. This is important to Customer Data security, because it serves to: properly report and retain documentation for events, begin remediation, discover root causes, learn lessons, and prevent similar occurrences (this is one way continuous improvement is supported).

IBM maintains a common single security incident reporting and mitigation system in which IT security and data incidents which may involve a compromise of: (i) either personal information, client information, IBM confidential, technical or scientific information, or (ii) a productivity device, or (iii) suspicious IT activity, or (iv) a suspected system penetration are reported to a single phone/web contact point. This report initiates a response from a 24x7x365 team of specifically trained and equipped employees who, working with the software business teams and other subject matter experts as needed, will manage the incident until resolution.

Subject matter incident responders have been identified for each software business area, so if an incident involves a software team, a security incident handling process (SIHP) is also invoked to ensure that a rapid, local business-unit response to security incidents, aligned with corporate reporting requirements, takes place for IBM's software business.

6. Employment Practices Related to Data Security

Protecting Customer Data depends on technical and other means as described earlier, and on the workforce that manages the data. Employment practices are designed to make sure that all employees and contractors meet a set of guidelines and can be, to the extent consistent with applicable law, monitored in their work-related activities.

Certain job classifications require extra security measures. For example, employees with user IDs on network infrastructure devices require quarterly employment verification.

Hiring and Separation Policies

Where permitted by law, pre-employment screening includes background checks, verification of claimed educational status, verification of government issued photo ID, and verification of other employment application claims.

Separation policies require removal of network access (target less than 24 hours).

Separating employees are required to return IBM property including workstations, laptops, IBM owned media, and any communication equipment. Separating employees are reminded of their continued obligation to data confidentiality.

Training and Culture

New employees receive training, which includes proper use of IT assets and protection of sensitive data. Annual CIO specified training in digital threats and security is required of all employees.

Compliance with Policies

IBM maintains an Employee Code of Conduct including Business Conduct Guidelines (BCG). These are administered by the IBM General Counsel. The BCG require that IBM'ers conduct business using high ethical standards and in accordance with data security and confidentiality policies. Employees are encouraged to report illegal or unethical behavior or even the appearance of it.

Employees must read and agree to abide by the BCG upon hiring and every year thereafter. Compliance with the BCG is a condition of employment. IBM makes the BCG available publicly at: http://www.ibm.com/investor/governance/business-conduct-guidelines.wss

Confidentially Speaking

In order to protect Customer Data, employees must feel free to bring problems to management attention at any time. IBM has established programs to enable this freedom to identify and report any potential issue.

The Confidentially Speaking program, formerly titled IBM Speak Up, was established decades ago, and enables IBM employees to express their concerns, whether related to their own job (e.g., benefits, careers, safety) or to an alleged violation of IBM's Business Conduct Guidelines (e.g., allegations of fraud, theft, improper business practices, circumvention or override of controls), or any other ethical issues. Since the program's founding, submitters' identities have remained confidential, known only to the administrator. To maintain the program's integrity, no one else is told who the submitter is, even those investigating the submission, without the submitter's permission. This degree of anonymity is intended to remove inhibitions to reporting potential issues.

In addition to the Confidentially Speaking program, other programs enable any employee to voice concerns about business practices or any safety or ethical issues at any time.

These programs enable any employee with concerns about Customer Data handling to bring them to appropriate management attention.

To further enhance employee's willingness and comfort in reporting any deviation from proper business practices, IBM maintains a formal position against any form of retaliation against any employee voicing safety, ethical, legal, or other concerns. No form of retaliation is tolerated and this fact is part of employee training and memorialized in the BCG.

7. Corporate Controls, Corporate Instructions, CIO Standards

The “tone from the top” and corporate direction to customer service and protection of assets including Customer Data is communicated through official means, which are discussed at high level in this chapter.

IBM uses the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework and its five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring.

IBM has a long-standing history for establishing, formalizing and communicating the fundamental key values that comprise IBM’s controls framework. IBM’s Organization Manual states
“IBM’s policies reflect the company's chosen value system within which decisions are made; they express the things that are fundamental, basic, most important, and therefore most enduring.”

IBM policies govern actions within IBM and its external relationships.
Policies and uniform practices are established in the form of Corporate Directives which are IBM’s primary method for documenting and effectively communicating its policies, delegations, and instructions to IBM management and employees. Directives are announced in a variety of formats, including policy letters, organization letters, and corporate instructions (CI). They are supported by a global administrator and a set of defined General Guidelines which describe the process by which the authorities are created, revised, or rescinded. IBM also utilizes standards and accounting practices to communicate policy and procedural requirements.

IT Security policies derive their authority from specific CI’s and other authoritative business control sources as above and as such are an integral part of IBM’s business.
CI’s have established IT standards and these have been created by the CIO organization. Compliance with these internal IT standards is mandatory at every level and audited. The standards themselves cover every aspect of IT.

Deviations

Any deviations from standard security policies or procedures must be applied for, documented, approved by management, and remediated as appropriate. The deviation documentation is required to be kept according to policies set in IBM Worldwide Records Management.
In addition, any deviation from a security policy must have secondary controls put in place and the deviation must be rectified within a specified timeframe. All deviations are tracked and reported until resolved.

8. Audit

Customer Data security depends on controls being implemented and verified. One way verification is achieved is through audits independent of the unit performing work.

IBM routinely audits for compliance with business controls, including IT controls (auditing that security standards and policies are in fact in compliance). The Business Controls and Internal Audit function report to the IBM CFO, who is accountable to the Audit Committee of the Board of Directors.

IT audits are performed to insure a variety of internal standards are being followed. The IT standards cover network, server, workstation, and applications among other things as described earlier. Auditors are separate from all areas they are responsible for auditing, following the Separation of Duties security principle.

Management self audits are performed and serve as an additional layer of control verification.

9. Business Continuity

One aspect of Customer Data security is data availability (given proper authorization). Key data, if unavailable, is useless and may prevent important business functions from continuing. For example, the provision of service and support to customers is a critical business function and can depend on availability of Customer Data provided by IBM customers.

All functions critical to the operation of IBM's business have disaster recovery (DR) plans. These formal plans are documented and annually (at least) revalidated. Software problem reporting and resolution services, which depend on Customer Data, are critical and have DR plans.

Preventing disruptions to services due to malware (logical intrusion) or physical intruders is covered in other chapters.

In the case of IBM SaaS offerings, the individual Security Practices statements for the offering in question have a description of the specific procedures and technologies applicable to that offering.

Crisis Management

IBM maintains a Crisis Management process under an Emergency Planning Program, designed to enable IBM to address crises as they arise. The process requires IBM sites/locations with personnel to create an Emergency Plan. The Crisis Management process is activated immediately when an actual or potential crisis situation arises.

The Crisis Management process requires each site to create a site emergency plan, which in turn requires the creation of a designated Crisis Management Team (CMT). In the event of an emergency, the Crisis Management Team convenes to assess the situation and develop an appropriate response. The Crisis Management Team (CMT) is chaired by a designated line manager or executive, called the "Senior Location Executive" (SLE). The CMT is composed of designated team members, typically representing key functions, such as: Human Resources, Legal, Security, Integrated Health Services, Real Estate/Facilities, Finance, Communications and business units. The composition of the local CMT will differ depending on the size of the site. Other team advisors can be brought in as needed.

In addition to site CMTs, IBM maintains a Corporate Crisis Management Team (CCMT) designed to address disasters that impact a meaningful segment of our business operations. The mission of the

CCMT is to efficiently communicate and coordinate support information for a wide variety of emergencies with specific focus on the well-being of employees, safeguard of assets and assist with the recovery of business operations.

10. Acquisitions

From time to time, IBM may acquire other companies with existing Customer Data security policies and procedures that differ from IBM's. Acquired companies are required to comply with the same security policies as the rest of IBM within a defined integration or transition period after the acquisition. The same physical, logical, and business controls that are applied across IBM will apply to the acquired company by the end of the integration period.

The length of time required for the integration period depends on an assessment of the complexity of the acquired company's existing infrastructure.

For an acquisition, an integration team is formed, headed by an appointed Integration Executive, with members from IBM and the acquired company. The team will consist of IT security experts; business controls experts, finance, HR, and other key business functions. Physical and logical security reviews and assessments are performed by the integration team as a matter of priority, augmented by outside experts as required. Prior to the completion of the integration, the practices stated herein do not apply to the acquired company.

11. Service and Support

Customers may be asked to provide data to aid in debugging a problem. This is Customer Data as described in this document and described further in the service and support resources below. Customers may be asked to use the ECuRep (Enhanced Customer Data Repository) online tool to send debugging data to IBM. The Ecurep tool and its terms of use are described here: http://www.ibm.com/de/support/ecurep/index.html.

Note: Customers have the option of securely transporting (i.e., encrypting through secure HTTP or secure FTP) data electronically sent to IBM.
In addition, the IBM Software Support Handbook provides details:
http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html 20

If a customer sends IBM hardcopies, or other physical media such as tapes, physical security guidelines are followed. Further information concerning hardcopies is contained in the two web accessible sources listed above.