cci
Career Connection
Incorporated

Career Connection, Inc.
Data Privacy Guidelines

Objectives

This course is intended for CCI employees. The course gives guidance on data privacy concepts and describes how data privacy is relevant when delivering services for IBM and for clients.

At the conclusion of this course, you should be able to:

- Define key terms such as: *Personal Information* and *Sensitive Personal Information*
- Identify data privacy concepts that apply to delivering services for clients and IBM worldwide
- Identify data privacy concepts that relate to the handling of personal information
- Differentiate between CCI's personal information and the client's personal information
- Describe the importance of adhering to data privacy requirements imposed by law
- Identify the circumstances under which you should ask for assistance when handling personal information
- Describe when to report a data privacy incident

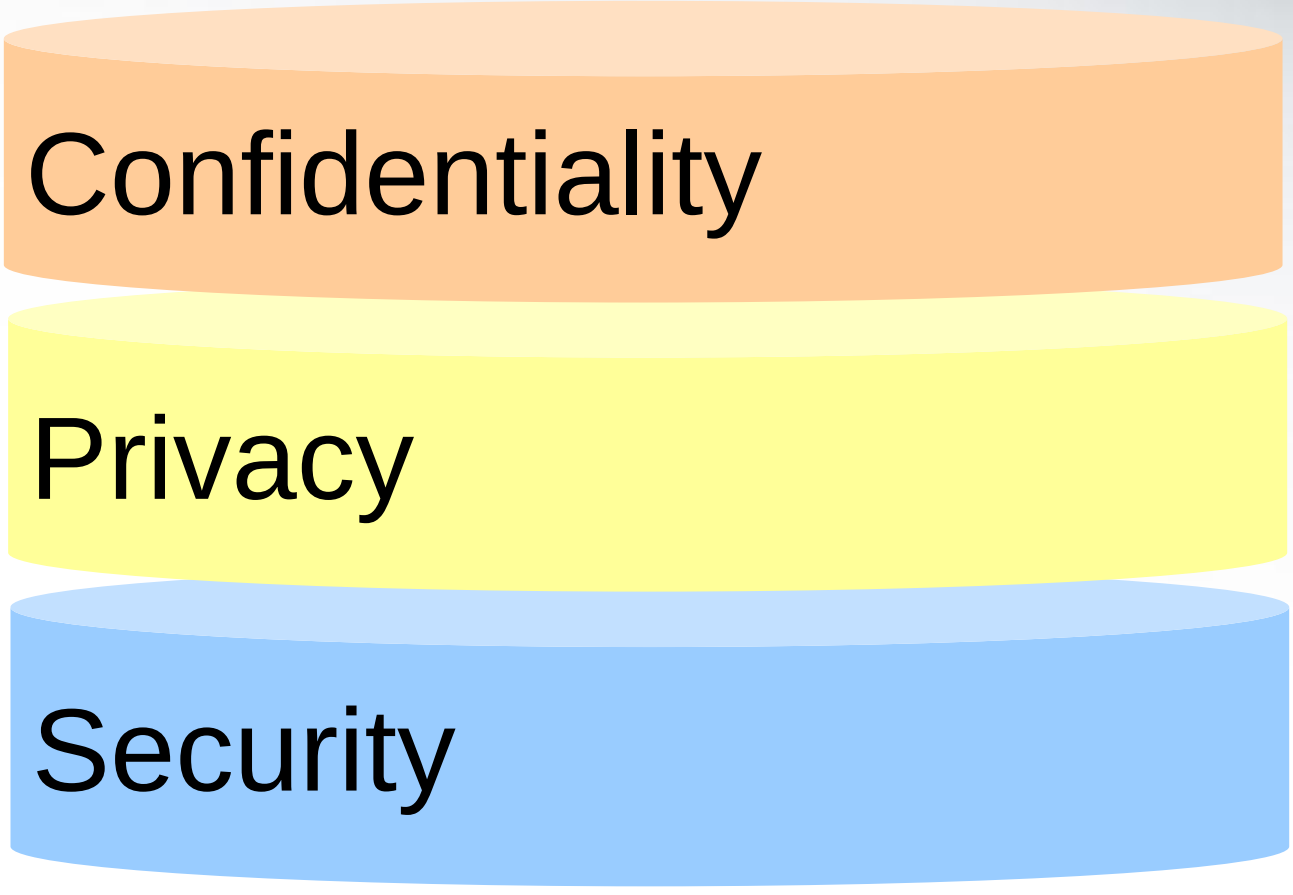
Data Privacy and Protection

It is critical that we raise awareness of the way in which personal information (PI) and sensitive personal information (SPI) should be handled in the IBM environment.

Your Responsibility

- Privacy is every CCI employee's responsibility. In a world in which data is easily acquired, shared, and stored, and where concerns about potential data misuse emerge as a result, each of us must do our part to handle such information in compliance with the privacy requirements and values of the clients and of IBM.
- You have a responsibility as:
  - An employee
  - A manager
  - The owner or developer of a software application
  - The user of client or IBM data
  - A delivery employee
- Responsibility may arise:
  - When communicating within CCI or to external parties
  - When accessing data
  - When moving work
  - If data has been lost, misplaced, or compromised

Security, Privacy, and Confidentiality



Security versus Privacy

Security

- Security is about the **protection** of information.
- Security covers **all kinds** of information, not just information about individuals.
- Security is referred to in the context of **access to IT infrastructure and services**.
- Security is defined in terms of **access and disclosure rights**.

Privacy

- Privacy is about the **handling** of information.
- Privacy mostly covers **personal information;** about individuals, not entities.
- Privacy is often referred to in the context of **how business processes and practices are executed**.
- Privacy rights are determined by the **purpose of collection** of the information and the privacy policy.

Privacy versus Confidentiality

Privacy

- Privacy covers information about **individuals**.
- The **collector** determines the purpose of collection.
- Despite release, **privacy rights may remain**.
- It is **difficult to apply classification rules** to personal information.

Confidentiality

- Confidentiality covers information about **companies and individuals**.
- The **creator** determines the confidentiality of the information.
- **Confidentiality is lost** if the information is released.
- It is **easy to classify information** as confidential.

What is PI?

- Personal Information (or PI) is any information that identifies or can reasonably be used to identify the individual to whom such information pertains.
- PI includes publicly available data elements, for example:
  - Name
  - Home telephone number
  - Home address
  - Business contact information
- Clients may have different classifications and handling requirements for their PI.

What is SPI?

- Sensitive Personal Information (or SPI) is a special type of personal information that requires more careful handling.
  - Sensitive Personal Information may also be called Special Categories of Data or other terms that designate the sensitivity of the personal information.
- Some types of personal information are considered sensitive due to the legal considerations in many countries and/or the potential risks that such information could be misused to significantly harm an individual financially or personally.
  - CCI employees should not collect or retain sensitive personal information without checking on the legal requirements.
- SPI must receive a higher level of protection than PI that is not sensitive.
  - Check the client's requirements for handling SPI.

What is SPI? (cont'd)

- At CCI we always consider the following data elements to be SPI. An individual's:
  - Country identification number, such as Social Security Number (SSN), or other government-issued identification number such as driver's license or passport number
  - Bank account number
  - Credit card or debit card number
  - Health and medical information, including health insurance identification numbers
  - Date of birth, when the year is included
  - Racial or ethnic origin
  - Sexual orientation
  - Political opinion
  - Trade union membership
  - Religious or philosophical beliefs
  - Data concerning physical and mental health, including state of health, illness, disabilities, pathological defects, or medical treatments
  - Criminal records including convictions, decisions of penalties and fines, or other information collected in judicial or administrative proceedings to ascertain an offense or regarding an alleged or suspected commission of an offense
  - Biometric or genetic data
  - Social welfare needs or benefits or other social welfare assistance received

The Client's Personal Information

- There is a distinction between the client's Personal Information versus CCI's Personal Information:
  - The client will decide what personal information it collects from its customers and employees and the terms under which it collects that personal information.
  - The client will continue to have responsibility for its own personal information and will update and manage it accordingly.
  - The client will apply its own classification system to its own personal information.
  - The client will be subject to regulatory requirements in relation to its own personal information and its own data, generally.
  - CCI will be subject to the client's instructions in relation to the client's personal information and data, generally.
  - The client will apply its own practices and policies in relation to its own personal information.
- It is critical to understand this distinction because CCI employees manage the client's information on behalf of the client.

Fair Information Principles

The general principles are:

- **Accountability:** Collect, use, and disclose PI responsibly.
- **Fairness:** Collect and process PI fairly and lawfully.
- **Purpose:** Specify the purpose of collection and use it for that purpose.
- **Security:** Physical, technical, and organizational measures should be used to safeguard PI.
- **Accuracy:** Keep PI as accurate, complete, and up-to-date as is necessary for the purpose for which it is processed.
- **Disclosure:** PI should be disclosed appropriately.
- **Access:** Upon request, provide individuals with appropriate access to PI about them.
- **Retention and disposal:** PI should be kept only for as long as is necessary and appropriate.

Data Controller versus Data Processor

The controller

- **Is the custodian** of customers' PI and the process of collection
- **Sets the purpose** of collection of the information
- **Sets the data handling** requirements
- Is **often registered** with a relevant regulatory authority
- Is **responsible for a customer's access requests**

The processor

- Has **no direct relationship** with the client's customer
- Has **no knowledge of the purpose** of collection
- Handles information according to the data controller's requirements
- **May or may not need to be registered** with a regulatory authority
- Is **not responsible for access requests** and acts only on the instructions of the data controller

Privacy Is Every CCI Employee's Responsibility – It Starts and Ends with Every One of Us

- Personal information should be handled appropriately according to its classification.
- When communicating within IBM or to external parties, certain data protection rules must be followed.
- Sensitive information should not be collected unless the legal requirements are checked.
- Sensitive information should be properly protected, not be retained for longer than it is needed, and must be disposed of in a secure fashion.
- If there is suspicion that data has been lost, misplaced, or otherwise compromised, it should be reported immediately.

How are you handling PI?

- Look at the type of PI and the job that you do. You might be:
  - Using client PI to perform your job
  - Accessing PI
  - Transferring services to another location
  - Hiring a contractor
  - Running a team room
  - Archiving or retaining PI

Managing Client PI / SPI

- Instances where CCI employees handle PI or SPI on behalf of a client such as where we are a service provider and IBM is acting as a data processor, CCI employees will manage the 'client-owned' PI or SPI in its possession in accordance with the terms of IBM's contract with the client.
- Client-owned PI/SPI is subject to clients' requirements as opposed to our internal privacy policies and practices. The client will have their own privacy practices and policies.
- If the client wants IBM to implement certain privacy practices and policies they will need to be part of the contract or contained in an agreement with the client on privacy and security practices.

Policy Governing the Client's PI

- A traditional security statement may look like this:

  "Members of the ABC consulting team are allowed to access the client files."

- Incorporating the notions of privacy make us write a much more complex statement:

  "Members of the ABC consulting team are permitted to see the client files for the purpose of assessing the return on investment (ROI) of client process model and for other purposes only if client provides explicit permission (based on individual permissions granted to client, if needed)."

- Technology must help organizations articulate, enforce, and demonstrate compliance with these types of policies.

Workplace Security

- Line management is responsible to establish and enforce a workplace security process.
- The process must include testing and reporting of results.
- Disciplinary measures may be taken against repeat violators (up to and including dismissal).
- Workplace security should be a habit, not a process.
- Individuals are responsible for individual work areas.
- Violations must be reported to management.

What Is Covered?

- All confidential and sensitive material must be locked up or securely stored.
  - This includes personal materials.
- Ensure no keys are left out.
- Do not keep written passwords in your workstation area.
- Lock all drawers and cabinets.
  - Note that site workstation Health Checks may be performed at any time, including after hours.
- Mobile phones or personal devices must be secured.
  - All recording devices require management approval.
- All media (portable or otherwise) must be secured.
- Laptops should be secured using a Kensington lock (or equivalent).

Clean Desk Policy

- Appropriately secure the information in calendar invitations.
- Lock your laptop away or take it with you – do not leave it out unsecured.
- Enable screen saver and power on passwords on your laptop or desktop – do not leave your screen open and unattended.
- Dispose of confidential paper in the confidential disposal bin – do not leave it on the printer.
- Secure the Personal and Confidential Information of IBM, its clients, suppliers, and partners.
- Make sure Confidential Information is clearly labeled – control the distribution of hard copies and don't share Confidential Information.
- Lock your drawers, cabinets, and filing cabinets and secure your keys.
- Erase the white board – never display Confidential Information in public.
- Secure recordable media.

Reporting Data Incidents

- Incidents involving the loss or compromise of Personal Information (PI) can have serious negative consequences for IBM and its clients and must be handled appropriately and promptly.
- A data incident occurs when one has reason to suspect that PI/SPI has been lost, misused, stolen, disclosed, or accessed inappropriately. This includes instances where PI/SPI was stored on a laptop or any other portable media.
- It is crucial that any employee who suspects that PI/SPI may have been lost or compromised report it immediately.

What Would You Do?

1. You drive to a restaurant for lunch and have your laptop with you.
2. You save a spreadsheet of client data that includes names and Social Security Numbers on your laptop and on a "thumb drive."
3. You want to get a set of data to a vendor or partner and the easiest thing to do is send it via UPS or Airborne.
4. You have started a blog.
5. You manage several IT systems and want to share the workload with someone else.
6. You suspect that a laptop or data tape is missing.

What Would You Do?

1. You drive to a restaurant for lunch and have your laptop with you.
   Answer: Lock it in the trunk or take it with you.
2. You save a spreadsheet of client data that includes names and Social Security Numbers on your laptop and on a "thumb drive."
   Answer: Make sure it is encrypted or do not save it to portable media.
3. You want to get a set of data to a vendor or partner and the easiest thing to do is send it via UPS or Airborne.
   Answer: Use only approved methods to send Sensitive Personal Information—no overnight mail!
4. You have started a blog.
   Answer: You are cool! But do be careful what you post when it comes to IBM information and your own or someone else's information.
5. You manage several IT systems and want to share the workload with someone else.
   Answer: Do not share IDs or passwords.
6. You suspect that a laptop or data tape is missing.
   Answer: Report it!

Data Privacy Education Summary

You should now be able to:

- Define key terms such as: *Personal Information* and *Sensitive Personal Information*
- Identify data privacy concepts that apply to delivering services for clients at IBM
- Identify data privacy concepts that relate to the handling of personal information
- Differentiate between CCI's personal information and the client's personal information
- Describe the importance of adhering to data privacy requirements imposed by law
- Identify the circumstances under which you should ask for assistance when handling personal information
- Describe when to report a data privacy incident