Presentation User Guide

PURPOSE

- The purpose of this training is to provide the Global Business Services (GBS) practitioners with guidance on management of risk, BCP and overall protection of IBM's and our Client's personal information, sensitive personal information and business sensitive information on their engagements.

TARGET AUDIENCE

- IBM Workforce (including global resources)
- IBM Contractors
- IBM Sub-contractors

DELIVERY

- Deliver Data Security Privacy Training to project team members, including contractors and sub-contracts
- Suggestions for delivery include team meetings, on-boarding presentations, or team planning sessions
- Recommend delivery by Project Executive, Project Manager, or Team Lead

IBM Project Specific Training on bp *account*

IBM Services

IBM

AGENDA

Objective & Goal

Data Security & Privacy Definition

General Data Protection Regulation (GDPR)

Your Responsibility

Working From Home: Security and Privacy Practices

How to Handle PI/SPI/BSI data

Incident Reporting

Password & Username Best Practices

BP Security requirements

BCP Awareness

Essential Links

Conclusion

Objective & Goal

OBJECTIVE:

Data privacy is about the protection of personal information and the ability of an individual to have significant control over personal information that pertains to them.

GOAL:

To educate the IBM Workforce to comply with IBM DS&P policy and client security policy. We have introduced Account level DS&P Process with our on boarding deck which help our resources to understand how to handle PI & SPI, BSI Data.

Privacy and data protection is every IBMers responsibility.

Data Security & Privacy Definition

IBM's Global Data Security & Privacy Definition

Data Privacy: The ability of individuals to determine when, how, and to what extent information about them is used or disclosed to others.

Personally identifiable information (PI) includes any data element relating to identified or identifiable individuals

Sensitive personal information (SPI) could be misused to harm a person in a financial, employment or social way. [The USA also focuses on information facilitating identity theft (SSN, account code, PIN, etc.), and on medical information]

*IBM's definition of SPI can be found here.

Business sensitive information (BSI) is information protected by a client or other company as important to their business, the improper exposure or use of which could harm them.

Security: The practices we employ through people, processes and technology to protect information to minimize the potential of a data breach or security compromise

All IBM projects must follow foundational Data Security and Privacy standards and policies.

DS&P Risks with projects

Contracts are Sometimes Vague: Get agreement with client on which data security and privacy measures and roles/responsibilities to include in Release Orders.

Risk Management: Ensure risks are documented and managed

Human Understanding: Data breaches occur based on human error or out of lack of following procedures; team members are not educated on reporting incidents

Workforce access to PI/SPI/BSI: Workforce may have access to sensitive and confidential information.

- On/Off-Boarding: Not following the process of training new personnel or removing access to client systems when leaving project
- User Account Mgmt: There is not an approved written process to add, change and/or remove accounts timely and obtain appropriate approval; timely validation process for accounts in accordance with client policy
- Separation of Duties (SOD): The architecture and/or access control mechanisms allow for one individual to develop, test and access production (one person controls the complete cycle)

Monitoring: Monitoring of production environment not performed; monitoring of high risk functions not performed (for example, System Administrator and/or DBA activities)

Change Management: Software and data changes not tested prior to release in production; no Emergency access process that supports SOD for off-hours

Generic ID and Privileged Access: Not following the proper process while using Generic IDs and Privileged Access in the client system lead to a potential risk.

Importance of DS&P & GDPR

Key Factors:

- **IBM's Reputation**
- **Contractual Requirements**
- **Compliance with Global and Regional Regulations and Directives**
- **Client Relationships: "Trust"**

Contributing Factors:

- **Loss: Accidental, intentional**
- **Theft: Physical, logical**
- **Misuse: Employee, third party**
- **Disclosure: Inadvertent, inappropriate**
- **Access: Unauthorized**
- **Increasing Regulatory Requirements**

…. Also impact to individual persons

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR)

The EU General Data Protection GDPR:

Is the new General Data Protection Regulation that has been adopted by the EU and EEA.

It establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR impacts IBM and IBM's client contracts, policies and procedures when handling personal data.

GDPR brings for instance:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors
- Significant financial penalties for non-compliance
- Compulsory data breach notification

GDPR Link –

Enhanced protection for data subjects:

- Higher standards for obtaining consent
- Easier access to own personal data and insight into how it is processed
- Right to object to processing
  Right to request erasure – "right to be forgotten"
- Right to data portability
- Right to rectification

PI/SPI Lists

PERSONAL DATA LIST

Education and Professional Certifications
Profession and Employment Information
Professional Affiliations
Biometric
Criminal Records and Prosecutions
Demographic
Economic and Financial
Health and Medical Records

PROCESSING ACTIVITIES

Combines
Copies
Deletes
Hides
Links
Obscures
Parses
Reads
Receives
Sends
Shares
Stores
Transforms
Transitions
Updates

DATA SUBJECTS

Employees
Retirees
Temporary or casual workers
Applicants, pre-hires, other prospective employees
Consumers
Customers' Personnel
Personnel of Customers' Affiliates
Personnel of Customers' Business Partners
Personnel of Customers' Vendors
Business Partners' Personnel

SPECIAL CATEGORIES OF PERSONAL DATA(Sensitive Personal Data)

Criminal Convictions Status
Biometric Data
Ethnicity
Genetic Inheritance
Health Status
Individual Sex Life
Race
Religion
Religious Affiliation
Trade Union Membership Status

GDPR Obligations for Processors

Maintain Records

IBM has obligation to maintain written records of processing activities so it is important to keep Personal Data Inventory up to date

Technical & Organizational Measures

Appropriate Technical & Organisational Measures (TOMs) to protect personal data has been identified – to comply with them it's important that you **fulfil your responsibilities**

Personal Data Breach Reporting

IBM has responsibility to Inform and assist the Client in case of a personal data breach – ensure that you follow **Incidents reporting process.**

Data Processing Agreement

Data Processing Agreement with BP is in place, DPA is held on Master Service Agreement Level (MSA) and covers all work we do at BP

Data Protection Impact Assessment

IBM has obligation to assist BP with DPIA (which assess the privacy risks) – if you are requested to assist contact the management on the account for further guidance

Data Subject Rights

IBM has obligation to assist BP with their obligations towards the Data Subjects - if you are requested to assist contact the management on the account for further guidance

YOUR RESPONSIBILITY

General

Understand IBM policy and foundational Data Security and Privacy (DS&P) controls

- Certify completion of Data Security and Privacy training annually
  - Understand any BP-specific requirements for the project
  - Provide documentation of completed training to your management
- Adhere to Workplace Security policies identified to you

Understand the security and privacy requirements for the project

- Manage risks related to the handling of PI/SPI/BSI
- Report any inappropriate security risks that you have identified to your Project Manager
- Report any actual or suspected data breaches immediately to your Project Manager
- Make your work environment secure and apply DS&P controls to home and/or remote environments
- Contact your Project Manager for more information

Working From Home: Security and Privacy Practices

Essential Guidance:

Watch out for scams

"phishing emails“ that pretend coming from:

I. health authorities like the WHO
II. a national health service
III. news outlets
IV. great deals on purchases of articles that may be hard to get in the store
V. urgent requests for money transfers
VI. IT support calls

Pro tip: while the IBM cybersecurity team periodically sends out "phishing simulations" to measure how well you recognize this type of fake email, we pledge to never use COVID related themes in our tests.

Keep your devices updated

Accept and install the OS updates received for Windows 10 and Mac

Pro tip: set Microsoft AutoUpdate to automatically download and install Microsoft Office updates. On your mobile device, and on MacOS, configure your AppStore to automatically keep apps up to date.

Mind your browsing habits

Minimize the risk of compromise and avoid using your IBM device for personal recreational browsing as much as possible.

Pro tip: for personal internet use, use a personal device rather than the one you use for business

Essential Guidance:

Keep IBM and customer data secure

Don't use IBM applications from a device that's not approved for IBM business – that means only access your email from an approved device

Pro tip: never use your w3id credentials on a device that is not IBM managed

Keep client systems and networks secure

You should maintain the discipline of using the client-owned system for client work when working from home.

Pro tip: check with your manager before using your IBM device for client work rather than a client-owned system, as IBM issued devices may only be used as approved by the client

Don't let family or guests use your IBM device

Pro tip: many commercial computer games install "root kits" on the device that are intended to prevent cheating. They also hurt the security of the device by intercepting keystrokes and mouse movements. In many cases these "root kits" are indistinguishable from malicious software and may trigger alerts for our security team. Be smart, don't install games on your work device.

Be mindful of data privacy and confidentiality

Pro tip: put away confidential papers when you leave your desk and lock the screen of your device, even if you're just "stepping away" for a brief moment. If you can, use a headset for your Webex meetings and phone calls.

Essential Guidance:

Be smart about using IBM tools

Did you know that for many business applications you do not need to be connected to the IBM VPN? Email, Slack, Webex, Box, Workday – and even Your Learning – are all hosted in the Cloud and can be accessed without connecting to the VPN

Pro tip: use the Webex application rather than Webex in the browser for the best performance. If you have local network bandwidth issues, consider turning off video. When Voice-over-IP is not working properly, you can have call in or have Webex call you back on your phone for more consistent voice quality.

Wireless security

Pro tip: if you have administrative access to your router, check if you can update the firmware to the latest version. Also make sure you are using a secure administrator password. If possible in the router settings, disable remote administration so that only computers on your home network can manage the router.

Report incidents as quickly as possible

Report incidents to the CSIRT here: https://w3.ibm.com/cybersecurity/report.html.

How to Handle PI/SPI/BSI data

IBM Services

Your Responsibilities – Accessing PI/SPI/BSI

Manage User Accounts:

- Only use User IDs and passwords that are unique to you
- Do not share or disclose User IDs and passwords
- When changing assignments or roles, cancel in a timely fashion User IDs that are not needed

Manage Access to Environments:

- Only have access to PI/SPI/BSI that is required to perform your job and is authorized on a form
- Do not place or use real or live PI/SPI/BSI in test or development environments; this data must be masked, scrambled, or otherwise anonymized to mitigate risks
- The identified PI/SPI Information should be handle as per the defined guidelines.

Maintain a secure workplace and workstation:

- For workstation equipment assigned to you, physically protect it as appropriate, such as by using a locking cable
- Never leave PI/SPI/BSI unattended on your screen, on your system, or around your workspace
- Shut down or use password-protected screen savers at all times
- Secure printed material and portable media in locked desks and drawers
- Verify that your workstation and any equipment you control has the most current security updates, antivirus software and patch levels installed

Your Responsibilities – Storing & Disposing of PI/SPI/BSI

Avoid storing PI/SPI/BSI on portable devices and media as it is prohibited as per IBM Process:

- Pen Drives, USB Stick, External Hard disks and so on
- Hard copies

If you must use portable devices or media:

- Encrypt electronic data
- Store devices and media in a secure environment

Securely dispose of PI/SPI/BSI as soon as it is no longer required:

- Shred physical media (printed copies, floppy disks, CDs, and so on)
- Securely overwrite data stored on computers

PI/SPI downloads should be stored only in a single folder in their laptop and securely deleted when not anymore required

Appropriately dispose of data at the end of the project

Your Responsibilities – Transporting PI/SPI/BSI

When electronically transferring PI/SPI/BSI:

- Encrypt PI/SPI/BSI data or use industry standard security protocols

When physically transferring PI/SPI/BSI:

- Limit distribution to people on the access control list
- Use appropriate controls:
  - Encryption, transportation over secure lines, or hand delivery.

When faxing PI/SPI/BSI:

- Use appropriate controls:
  - Do not leave PI/SPI/BSI unattended
  - Include a cover letter addressed to the receiver
  - Verify that the receiving machine is in a secure location
  - Inform the receiving party before faxing

Your Responsibilities – Using PI/SPI/BSI

Data entered into supporting tools can create issues with PI/SPI/BSI that are not obvious:

- PI/SPI/BSI entered into free-form text areas must comply with contractual and regulatory requirements, and should be avoided if possible
- People without authorization to view data may have access to all the data in a tool, including the data in question

Be careful not to include PI/SPI/BSI when entering data into documents created in support of a project, for example:

- Spreadsheets
- Text documents
- Notes
- Emails
- Screenshots / bitmaps

INCIDENT REPORTING

IBM Services

IBM

Incident Reporting

We depend on IBMers like you to report security incidents involving IBM employees, IBM contractors, IBM clients and IBM assets. These incidents may include theft, threats, acts of violence and vandalism. One has also need to report cybersecurity incidents, data losses, potential or actual data breaches, inadvertent data disclosures, viruses and telephone requests for IBM business sensitive information..

Assets to be protected are the following:

- Workstations used by GBS Workforce Members
- Client data managed or accessed by IBM
- IBM data
- IBM printed PI/SPI/BSI and confidential information
- Client printed PI/SPI/BSI
- Any storage device storing the above information
- Databases, code and applications

Misplacement, loss or theft of IBM or Client assets or data must be reported immediately to the Project Manager. The Project Manager will work with the Project Executive to immediately:

- Report the loss or theft of IBM and Client assets according to the IBM IT Security Standard
- Report the loss or theft of IBM or Client data according to the IBM Data Incident Reporting process:
- Follow the guidance of the GBS Data Incident Manager for all steps involved in resolving the incident

Link to report incidents: https://pages.github.ibm.com/ciso-psg/main/standards/itss.html#102-incident-reporting

Password & Username Best Practices

IBM Services

Password & Username Best Practices

Choosing a strong password is the first line of defense in securing personal and business data

Do not share your user id & password with anyone for any reason or for the ease of operations.

Immediately change the password for your user id once your manager/ colleague shares the password over mail.

Avoid sending password over mail

Do not write your password down or store it in an insecure manner.

Change your password every 90 days

BP Security requirements

IBM Services

BP security requirements -1-

Data Classification

"BP Information" means data or records of whatever nature and in whatever form held by, or under the control of BP and supplied, transferred or disclosed by or on behalf of BP to the Supplier relating to the business, clients, potential clients, employees, operations or otherwise relating to the business of BP

"General" means BP Information that would not cause significant harm, financial loss or embarrassment to BP or its employees if compromised. It can be shared with anyone in BP and contracted business partners at the discretion of the Information Owner. This classification was previously known as "BP Internal";

"Confidential" means BP Information that if compromised could cause disruption, financial loss or embarrassment to BP, its employees or business partners;

"Secret" means BP's most valuable information that is of such value or sensitivity that if compromised it could affect BP's ability to operate, directly affect BP's share price or cause serious damage to BP's global reputation.

BP security requirements -2-

IBM's user working for BP account shall:

-complying with the policies and guidance provided by BP;
-handling BP Information in accordance with its classification and keeping information and equipment secure;
-only accessing and sharing BP Information where authorised to do so and have a clear business need;
-not using BP Information, IT systems or services to make personal gains or to run or support a private business;
-not leaving Confidential or Secret BP Information on answering machines or voicemail;
-not disclosing BP Information externally, including when using the internet, social media, external social networks, instant messaging or blogging sites;
-not using personally owned devices to capture images of BP Information;
-maintaining the security of BP provided IT equipment by not downloading any unauthorized software or programs, illegitimate files or email attachments;

PASWORD -3-

Passwords shall:

- be a minimum of eight (8) characters long
- include a combination of at least three (3) of the following:
  - numbers;
  - upper-case letters
  - lower-case letters;
  - special characters
- not be the same as any of the previous twelve (12) passwords used.

Privileged account and service account passwords shall:

- be a minimum of fourteen (14) characters long;
- include a combination of at least three (3) of the following
  - numbers;
  - upper-case letters;
  - lower-case letters;
  - special characters
- not be the same as any of the previous 12 passwords used

BCP (Business Continuity Plan) Awareness

IBM Services

General

Understand IBM BCP Concepts

Understand the IBM BCM Awareness Training

Essential Links

IT Security Standard	IT Security Standard at IBM
BCG	Business Conduct Guidelines –Mandatory for all employees to read, understand and comply
Data Privacy	GBS Data Security & Privacy Guidance
IT Security portal	Gateway to the whole lot of information about IBM IT Security policies, guidelines, standards, best practices
IBM Standard Software Installer (ISSI)	Contains software catalog, which can be installed for business purpose
Incident reporting	GBS Business Information Security Office Corporate Security

Conclusions

- Understand your requirements regarding PI/SPI/BSI
- Use good security practices at all times
- Key areas to focus on include:
  - Protection of PI, SPI, and BSI
  - Management of access to systems and environments
  - Separation of duties
- Minimize risk associated with access to PI/SPI/BSI

Manage expectations

One final note: No one answer fits every situation

- Ask yourself how best to handle and protect the data you are responsible for
- Be aware of the requirements associated with that data
- Think

THANK YOU!