INFORMATION SECURITY POLICY

sbPowerDev

First Drafted and Implemented for sbPowerDev, India:
31st January 2021

Revised to Include sbPowerDev, Singapore:
1st April 2023

Revisions and Updates:
31st January 2022
31st January 2023
1st April 2023
31st January 2024

Any queries / concern regarding policy should be sent to
contactus@sbpowerdev.com

Contents

INFORMATION SECURITY POLICY

1. Introduction

sbPowerDev is committed to safeguarding its information assets and ensuring the confidentiality, integrity, and availability of data. This policy establishes a framework for managing information security within our organization, focusing on practical measures and responsibilities.

2. Scope

This policy applies to all employees, contractors, and third-party partners of sbPowerDev, covering all information assets, systems, networks, and data owned or operated by the company.

3. Information Security Objectives

- **Confidentiality:** Ensure that information is accessible only to those authorized to have access.
- **Integrity:** Safeguard the accuracy and completeness of information and processing methods.
- **Availability:** Ensure that authorized users have access to information and associated assets when required.

4. Roles and Responsibilities

4.1 Core Team (Administrators & Policy Implementors)

- **Develop and Implement Policies:** Establish and maintain the Information Security Policy and related procedures.
- **Conduct Risk Assessments:** Regularly assess risks and implement mitigation strategies.
- **Monitor Compliance:** Ensure compliance with security policies and report incidents to senior management.
- **Provide Training:** Conduct security awareness training and education programs.

4.2 Employees and Contractors

- **Comply with Policies:** Follow all security policies and procedures as outlined in this document.
- **Report Incidents:** Immediately report security incidents and vulnerabilities to the Core Team.
- **Participate in Training:** Attend security training and stay informed about best practices.

4.3 Third-Party Partners

- **Adhere to Policies:** Comply with sbPowerDev's security policies and procedures.
- **Protect Shared Data:** Ensure that data shared with third parties is protected according to sbPowerDev's standards.
- **Cooperate with Audits:** Participate in security assessments and audits as required.

5. Information Security Management

5.1 Risk Assessment

- Conduct regular risk assessments to identify and evaluate potential threats and vulnerabilities.
- Develop and implement risk mitigation strategies to address identified risks.

5.2 Access Control

- **User Authentication:** Implement strong password policies and multi-factor authentication where applicable.
- **Access Rights:** Limit access to information and systems based on job roles and responsibilities.
- **Regular Review:** Conduct regular reviews of access rights to ensure compliance with security policies.

5.3 Data Protection

- **Encryption:** Use encryption to protect sensitive data both in transit and at rest.
- **Data Classification:** Classify data according to its sensitivity and implement appropriate protection measures.
- **Data Loss Prevention:** Implement measures to prevent unauthorized access, alteration, or destruction of data.

5.4 Incident Management

- **Incident Reporting:** Establish a process for reporting security incidents promptly.
- **Response Plan:** Develop and maintain an incident response plan to address security breaches and minimize their impact.
- **Continuous Improvement:** Conduct post-incident reviews to identify lessons learned and improve security measures.

6. Compliance and Monitoring

- **Legal Compliance:** Ensure compliance with applicable laws, regulations, and industry standards related to information security.
- **Regular Audits:** Conduct regular security audits and assessments to identify vulnerabilities and areas for improvement.
- **Policy Review:** Review and update the Information Security Policy annually or as needed to reflect changes in the security landscape.

7. Training and Awareness

- **Regular Training:** Provide regular security training and awareness programs for all employees.
- **Phishing Awareness:** Educate employees about phishing attacks and how to recognize suspicious emails and links.
- **Policy Updates:** Communicate updates to security policies and procedures regularly.

8. Enforcement

- Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.
- All employees and partners are expected to comply with the policy and report any suspected violations promptly.

9. Governing Law

This policy shall be governed by and construed in accordance with the laws of India and Singapore, where applicable.

10. Appendices

- Appendix A: Password Management Policy
- Appendix B: Data Classification Guidelines
- Appendix C: Incident Response Plan
- Appendix D: Access Control Procedures
- Appendix E: Mobile Device and Remote Work Policy
- Appendix F: Acceptable Use Policy
- Appendix G: Email and Communication Policy
- Appendix H: Change Management Policy
- Appendix I: Client Resource/Data Management Policy

APPENDIX A: PASSWORD MANAGEMENT POLICY

A.1 Purpose

The Password Management Policy aims to establish a secure environment by enforcing strong password practices for all users of sbPowerDev's systems and applications, leveraging Microsoft 365 and Windows 10 Pro capabilities.

A.2 Password Requirements

- **Complexity:** Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters (e.g., !, @, #, $).
- **Length:** Passwords must be at least 12 characters long.
- **Expiration:** Passwords must be changed every 90 days.
- **Reuse:** Previously used passwords cannot be reused for at least the last five password changes.

A.3 Password Management in Microsoft 365

A.3.1 Enforcing Password Policies

1. **Access the Microsoft 365 Admin Center:**
    - Go to admin.microsoft.com and log in with administrator credentials.
2. **Navigate to Security & Compliance:**
    - Go to **Admin centers** > **Security & Compliance**.
3. **Set Password Expiration Policies:**
    - Go to **Security** > **Identity & access management**.
    - Click on **Password policy**.
    - Set the password expiration period to 90 days.
    - Enable password history to prevent reuse of the last five passwords.
4. **Enable Multi-Factor Authentication (MFA):**
    - Go to **Users** > **Active users**.
    - Select the users to apply MFA and click on **Manage multi-factor authentication**.
    - Enable MFA for selected users to enhance security.

A.3.2 Managing Passwords on Windows 10 Pro

1. **Access Local Security Policy:**
    - Press Windows + R, type secpol.msc, and press Enter.
    - Navigate to **Account Policies** > **Password Policy**.

2. **Configure Password Settings:**
    - **Enforce password history:** Set to 5 passwords remembered.
    - **Maximum password age:** Set to 90 days.
    - **Minimum password length:** Set to 12 characters.
    - **Password must meet complexity requirements:** Enable this setting.
3. **Enable BitLocker for Additional Security:**
    - Go to **Control Panel** > **System and Security** > **BitLocker Drive Encryption**.
    - Turn on BitLocker for the system drive and configure it with a secure password or PIN.

APPENDIX B: DATA CLASSIFICATION GUIDELINES

B.1 Purpose

The Data Classification Guidelines provide a framework for classifying and handling data based on its sensitivity and importance, ensuring that appropriate security measures are applied using Microsoft 365 tools.

B.2 Data Classification Levels

1. **Confidential:**
    - Highly sensitive data that requires strict access controls.
    - Examples: Financial records, client data, proprietary information.
2. **Internal:**
    - Information intended for internal use only.
    - Examples: Internal memos, internal reports, internal project documents.
3. **Public:**
    - Information that can be freely shared with the public.
    - Examples: Marketing materials, press releases, public announcements.

B.3 Implementing Data Classification in Microsoft 365

B.3.1 Setting Up Sensitivity Labels

1. **Access the Microsoft 365 Compliance Center:**
    - Go to compliance.microsoft.com and log in with administrator credentials.
2. **Create Sensitivity Labels:**
    - Navigate to **Solutions** > **Information protection** > **Labels**.
    - Click on **+ Create a label** and define labels for each classification level (e.g., Confidential, Internal, Public).
3. **Configure Label Settings:**
    - **Confidential:** Restrict access to specific users/groups, apply encryption, and watermark documents.
    - **Internal:** Apply default access restrictions and track document usage.
    - **Public:** Allow open access with no additional protection.
4. **Publish Sensitivity Labels:**
    - Go to **Label policies** and click on **+ Publish labels**.

- Select the created labels and assign them to the appropriate users/groups.

B.3.2 Data Classification on Windows 10 Pro

1. **Using File Explorer for Manual Classification:**
   - Right-click on a file/folder, select **Properties**, and use custom tags to label data.
   - Use the **Details** tab to add metadata that reflects the data classification level.
2. **Enable Windows Information Protection (WIP):**
   - Go to **Settings** > **Update & Security** > **Windows Security** > **App & browser control**.
   - Configure Windows Information Protection to restrict access to specific applications and files based on classification.

APPENDIX C: INCIDENT RESPONSE PLAN

C.1 Purpose

The Incident Response Plan outlines procedures for identifying, responding to, and recovering from security incidents, ensuring minimal impact on sbPowerDev's operations.

C.2 Incident Response Phases

1. **Preparation:**
    - Conduct regular training and drills.
    - Maintain an inventory of critical assets and their security measures.
2. **Identification:**
    - Use monitoring tools to detect anomalies.
    - Analyze logs from Microsoft 365 and Windows Defender for suspicious activities.
3. **Containment:**
    - Isolate affected systems to prevent further damage.
    - Use Microsoft Defender ATP to quarantine threats.
4. **Eradication:**
    - Remove malware and unauthorized access.
    - Apply security patches and updates.
5. **Recovery:**
    - Restore systems to normal operation.
    - Use backups to recover lost data.
6. **Lessons Learned:**
    - Conduct post-incident reviews.
    - Update policies and training based on findings.

C.3 Tools and Procedures

- **Microsoft Defender ATP:** Monitor and respond to threats across devices.
- **Azure Security Center:** Analyze security alerts and recommendations.
- **Security Information and Event Management (SIEM):** Collect and analyze security data.

APPENDIX D: ACCESS CONTROL PROCEDURES

D.1 Purpose

The Access Control Procedures establish guidelines for managing access to sbPowerDev's systems and data, ensuring only authorized individuals have access.

D.2 Access Control Principles

- **Least Privilege:** Grant users only the access necessary to perform their job functions.
- **Separation of Duties:** Divide tasks and privileges among multiple users to prevent fraud and errors.

D.3 Implementing Access Controls in Microsoft 365

D.3.1 Managing User Access

1. **Access the Microsoft 365 Admin Center:**
    - Go to admin.microsoft.com and log in with administrator credentials.
2. **Manage User Roles:**
    - Navigate to **Users** > **Active users**.
    - Assign roles based on job responsibilities, such as Global admin, Exchange admin, etc.
3. **Configure Conditional Access Policies:**
    - Go to **Azure Active Directory** > **Security** > **Conditional Access**.
    - Create policies to enforce MFA and restrict access based on location or device.

D.3.2 Access Control on Windows 10 Pro

1. **Local Group Policy Editor:**
    - Press Windows + R, type gpedit.msc, and press Enter.
    - Navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.
2. **Define User Access Rights:**
    - Specify rights and privileges for local users and groups.
    - Use the **Security Options** to enforce password policies and account lockout settings.

APPENDIX E: MOBILE DEVICE AND REMOTE WORK POLICY

E.1 Purpose

This policy outlines the security measures for using mobile devices and remote work environments to protect company data.

E.2 Mobile Device Security

- **Device Encryption:** Ensure all company-issued mobile devices are encrypted.
- **Mobile Device Management (MDM):** Use MDM solutions to enforce security policies on mobile devices.
- **Application Restrictions:** Limit the installation of unauthorized applications.

E.3 Remote Work Security

- **Secure Connections:** Require the use of VPNs for remote access to company networks.
- **Static IP Usage:** Use static IPs to control access to client networks.
- **Data Protection:** Ensure that data accessed remotely is protected by encryption and secure connections.

E.4 Implementing Remote Work Security

1. **VPN Setup:**
    - Configure VPNs on Windows 10 Pro devices for secure access to internal systems.
2. **Use of Microsoft 365 Security Tools:**
    - Enable security features such as Conditional Access in Azure AD for secure remote login.
    - Monitor access logs for unusual patterns.
3. **Remote Work Best Practices:**
    - Educate employees on securing their home networks and devices.
    - Regularly review and update remote work policies.

APPENDIX F: ACCEPTABLE USE POLICY (AUP)

F.1 Purpose

The Acceptable Use Policy (AUP) establishes guidelines for the appropriate use of sbPowerDev's information technology resources, including computers, networks, email, and other electronic communication systems. This policy aims to protect the company's assets, ensure compliance with legal and regulatory requirements, and maintain a productive work environment.

F.2 Scope

This policy applies to all employees, contractors, and third-party partners who have access to sbPowerDev's information technology resources. It covers all devices, networks, and communication systems owned or operated by the company.

F.3 Acceptable Use

- **Authorized Access:** Users must only access systems and data for which they have explicit authorization. Access credentials, such as passwords, must be kept confidential and not shared with others.
- **Company Resources:** Use company IT resources primarily for business-related purposes. Limited personal use is permitted as long as it does not interfere with job performance or violate any company policies.
- **Software and Applications:** Only use authorized software and applications on company devices. Unauthorized software or applications that may pose security risks are prohibited.
- **Data Protection:** Protect sensitive data by adhering to data classification guidelines and using appropriate security measures, such as encryption and access controls.
- **Network Usage:** Use company networks responsibly, avoiding activities that could disrupt network performance or compromise security. This includes refraining from downloading large files unrelated to work, streaming non-work-related content, or engaging in peer-to-peer file sharing.

F.4 Unacceptable Use

- **Unauthorized Access:** Attempting to access systems, data, or resources without proper authorization is strictly prohibited.
- **Harassment and Discrimination:** Using company resources to harass, discriminate, or engage in any form of bullying is unacceptable.
- **Malware and Hacking:** Engaging in activities that introduce malware, viruses, or engage in hacking or other security breaches is strictly prohibited.
- **Inappropriate Content:** Accessing, downloading, or distributing content that is illegal, offensive, or inappropriate in a work environment is not allowed.
- **Data Manipulation:** Unauthorized alteration, deletion, or falsification of data is strictly prohibited.

F.5 Monitoring and Enforcement

- **Monitoring:** sbPowerDev reserves the right to monitor and review the use of its IT resources to ensure compliance with this policy. Monitoring may include tracking internet usage, email communications, and other activities conducted on company systems.
- **Enforcement:** Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual agreements. Legal action may be taken if activities are deemed criminal.

F.6 User Responsibilities

- **Compliance:** All users must comply with this policy and report any suspected violations to the Core Team or IT department immediately.
- **Training:** Participate in regular security and acceptable use training sessions provided by the company.

APPENDIX G: EMAIL AND COMMUNICATION POLICY

G.1 Purpose

The Email and Communication Policy outlines the proper use of sbPowerDev's email and other electronic communication tools. This policy ensures that communications are secure, professional, and aligned with company standards.

G.2 Scope

This policy applies to all employees, contractors, and third-party partners who use sbPowerDev's email and communication systems, including company-provided email accounts, instant messaging, video conferencing, and other communication tools.

G.3 Email Usage

- **Professional Use:** Use company email for business purposes. Personal use should be minimal and not interfere with work responsibilities.
- **Security:** Do not share sensitive or confidential information via email without using encryption or other security measures. Avoid clicking on suspicious links or downloading unknown attachments.
- **Email Etiquette:** Maintain a professional tone in all email communications. Avoid using offensive or inappropriate language and respect confidentiality.
- **Attachments:** Only open attachments from trusted sources. Report any suspicious emails to the IT department immediately.

G.4 Instant Messaging and Video Conferencing

- **Appropriate Use:** Use instant messaging and video conferencing tools for business-related purposes. Maintain professionalism during all communications.
- **Security Measures:** Ensure that communications are conducted over secure channels. Use passwords and encryption when required.
- **Recording:** Do not record video conferences or chats without the consent of all participants.

G.5 Social Media and Public Communications

- **Representation:** When representing sbPowerDev on social media or public platforms, adhere to company guidelines and maintain professionalism.
- **Confidentiality:** Do not disclose confidential or proprietary information on social media or other public forums.
- **Personal Views:** Clearly distinguish personal views from those of the company when posting on social media platforms.

G.6 Monitoring and Enforcement

- **Monitoring:** sbPowerDev reserves the right to monitor email and communication tool usage to ensure compliance with this policy.

- **Enforcement:** Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.

G.7 User Responsibilities

- **Compliance:** Adhere to this policy and report any breaches or concerns to the IT department.
- **Training:** Participate in training sessions related to secure and appropriate communication practices.

APPENDIX H: CHANGE MANAGEMENT POLICY

H.1 Purpose

The Change Management Policy establishes a structured approach to managing changes to sbPowerDev's information systems, applications, and processes. The goal is to ensure that all changes are reviewed, approved, implemented, and documented in a controlled manner to minimize risks and disruptions.

H.2 Scope

This policy applies to all changes to sbPowerDev's IT infrastructure, including hardware, software, networks, and applications. It covers changes initiated by employees, contractors, and third-party partners that may impact company operations.

H.3 Change Management Process

The change management process at sbPowerDev consists of the following key steps:

1. **Change Request Submission:**
    - **Initiation:** Any change must be initiated by submitting a Change Request (CR) form, detailing the change's nature, purpose, and potential impact.
    - **Documentation:** The CR must include a comprehensive description of the change, reasons for the change, and potential risks involved.
2. **Change Evaluation:**
    - **Impact Analysis:** The IT department or relevant team conducts an impact analysis to assess potential effects on existing systems, processes, and security.
    - **Risk Assessment:** Evaluate potential risks associated with the change and develop mitigation strategies.
3. **Change Approval:**
    - **Review Committee:** A Change Advisory Board (CAB) or designated review committee evaluates the CR, considering the impact and risks.
    - **Approval Decision:** The CAB grants approval, requests modifications, or rejects the change based on the evaluation.
4. **Change Implementation:**
    - **Preparation:** Prepare a detailed implementation plan, including timelines, resources required, and rollback procedures in case of failure.

- **Execution:** Implement the change following the approved plan, ensuring minimal disruption to operations.

5. **Testing and Validation:**
    - **Testing:** Conduct testing in a controlled environment to validate the change's effectiveness and identify potential issues.
    - **Validation:** Ensure that the change achieves its intended objectives without adversely affecting other systems.
6. **Post-Implementation Review:**
    - **Evaluation:** Review the change to ensure it has been implemented successfully and meets the desired outcomes.
    - **Documentation:** Update relevant documentation, including system records and user manuals, to reflect the change.
7. **Close Change Request:**
    - **Closure:** Officially close the CR, documenting all findings, lessons learned, and any follow-up actions required.
    - **Communication:** Notify all relevant stakeholders of the change's successful implementation and any new procedures or updates.

H.4 Roles and Responsibilities

- **Change Initiator:**
    - Submit detailed CR forms for proposed changes.
    - Participate in the evaluation and implementation phases as required.
- **Change Advisory Board (CAB):**
    - Review and evaluate CRs.
    - Approve, modify, or reject proposed changes based on impact and risk assessments.
- **IT Department:**
    - Conduct impact and risk assessments for proposed changes.
    - Implement approved changes and coordinate testing and validation.
- **System Owners:**
    - Ensure changes align with business objectives.

- Oversee the implementation and testing of changes in their respective areas.

H.5 Monitoring and Compliance

- **Continuous Monitoring:** Implement continuous monitoring to detect and address issues arising from changes.
- **Compliance Audits:** Conduct regular audits to ensure adherence to the Change Management Policy.
- **Reporting:** Maintain records of all changes, including approvals, implementation details, and outcomes.

H.6 Training and Awareness

- **Training Programs:** Provide training on change management processes to all employees involved in change initiatives.
- **Awareness Campaigns:** Conduct awareness campaigns to ensure understanding and compliance with change management procedures.

APPENDIX I: CLIENT RESOURCE/DATA MANAGEMENT POLICY

I.1 Purpose

The Client Resource/Data Management Policy outlines the measures sbPowerDev takes to ensure secure and protected access to client resources and data. The policy aims to safeguard client information, maintain data integrity, and ensure that client resources are used appropriately and securely, with a strong preference for not storing client data within sbPowerDev's environment.

I.2 Scope

This policy applies to all sbPowerDev employees, contractors, and third-party partners who have access to client resources and data. It covers all methods of accessing client information, including on-site, remote access, and cloud-based systems.

I.3 Key Principles

1. **Confidentiality:**
    - Ensure that client data is accessible only to authorized personnel and is protected from unauthorized access.
2. **Integrity:**
    - Maintain the accuracy and completeness of client data and protect it from unauthorized modification or destruction.
3. **Availability:**
    - Ensure that client data and resources are available to authorized users when needed.

I.4 Secure Access Measures

1. **Data Storage Preference:**
    - **Client Data Storage:** sbPowerDev prefers not to store any client data within its tenant. All client data should remain within the client's environment, protected by their security protocols.
    - **Microsoft Accounts:** Use Microsoft accounts to access and store data, leveraging Microsoft's security protocols.
2. **Access Control:**
    - **Client-Provided Credentials:** Use client-provided credentials with adequate and limited access to perform services. Ensure that all data remains within the client's environment.

- **Role-Based Access:** Grant access based on job roles and responsibilities. Implement the principle of least privilege to ensure users have the minimum access necessary to perform their duties.
- **Authentication:** Use mandatory multi-factor authentication (MFA) for accessing client resources. Ensure strong password policies are enforced, with client account passwords reset every 30 days and requiring strong alphanumeric passwords.

3. **Data Encryption:**
   - **In Transit:** Encrypt all data transmitted between sbPowerDev and client systems using TLS/SSL or equivalent protocols.
   - **At Rest:** Encrypt client data stored on sbPowerDev systems using industry-standard encryption algorithms (e.g., AES-256). Ensure all devices accessing client resources are encrypted with BitLocker on Windows Pro.
4. **Network Security:**
   - **Static IP/VPN:** Use static IP addresses or VPNs for accessing client networks based on client requirements and preferences.
5. **Endpoint Security:**
   - **Antivirus and Anti-Malware:** Ensure all devices accessing client resources are protected with up-to-date antivirus and anti-malware software.
   - **Device Management:** Use Microsoft Intune for managing and enforcing security policies on all company-issued devices.

I.5 Data Handling Procedures

1. **Data Classification:**
   - Classify client data based on its sensitivity and apply appropriate protection measures as outlined in sbPowerDev's Data Classification Guidelines.
2. **Data Minimization:**
   - Collect and retain only the minimum amount of client data necessary for business operations. Regularly review and securely dispose of data that is no longer needed.
3. **Data Sharing:**
   - Share client data only with authorized personnel and third parties who have a legitimate business need. Use secure methods for data sharing, such as encrypted emails or secure file transfer protocols.

I.6 Incident Response and Management

1. **Incident Reporting:**
    - Establish a process for promptly reporting security incidents involving client resources. Encourage employees to report any suspected breaches or vulnerabilities immediately.
2. **Response Plan:**
    - Develop and maintain an incident response plan to address security incidents involving client data. The plan should include steps for containment, eradication, recovery, and communication.
3. **Post-Incident Review:**
    - Conduct post-incident reviews to identify the root cause of security incidents and implement measures to prevent recurrence.

I.7 Compliance and Monitoring

1. **Legal and Regulatory Compliance:**
    - Ensure compliance with applicable data protection laws and regulations (e.g., GDPR, PDPA) when handling client data.
2. **Regular Audits:**
    - Conduct regular security audits and assessments to identify vulnerabilities and areas for improvement in the management of client resources.
3. **Policy Review:**
    - Review and update the Client Resource/Data Management Policy annually or as needed to reflect changes in security practices and regulatory requirements.

I.8 Training and Awareness

1. **Security Training:**
    - Provide regular security training for employees on best practices for handling client resources and data. Include topics such as secure access, data protection, and incident response.
2. **Awareness Programs:**
    - Conduct awareness programs to keep employees informed about the latest security threats and how to mitigate them.

I.9 Enforcement

1. **Policy Compliance:**

- All employees, contractors, and third-party partners must comply with this policy. Non-compliance may result in disciplinary action, up to and including termination of employment or contractual agreements.

2. **Monitoring and Reporting:**
    - Implement monitoring tools to track access to client resources and detect any unauthorized activities. Regularly review access logs and take appropriate actions to address any anomalies.