Privacy & Information Security Policy

At Evidence-Based Development International (Hereinafter: EBD International), safeguarding our clients' privacy and securing their information is paramount. We prioritize the confidentiality and protection of your personal information and organizational data, adhering unwaveringly to the highest standards of data protection. Our Privacy & Information Security Policy meticulously outlines:

A. the data we collect, how we utilize it, and what are our core privacy principles, as well as
B. the stringent measures we implement to ensure application of privacy and information security standards.

To ensure the effective application of the Privacy & Information Security Policy, all employees of EBD International and contracted consultants (both individuals and legal entities) must be informed, trained, and capable of fully implementing all aspects of this policy. To promote compliance and their accountability, they are required to sign a formal acknowledgment of the policy (See the form in Annex 2).

A: CORE PRIVACY PRINCIPLES AT EBD INTERNATIONAL

1. **Information and data we collect:**

    - In delivering our services, we primarily gather non-personal data, encompassing attitudes, knowledge, and thoughts, through the application of the highest ethical and scientific standards.
    - We collect and analyze organizational data (*Our understanding of organization's data is attached as Annex 1)*.
    - We may collect personal information such as name, email address, contact details, and professional affiliations when you engage with our services, including but not limited to inquiries, registrations, and transactions.
    - We may also collect non-personal information such as IP addresses, browser type, and device identifiers to improve our services and understand user preferences.

2. **How we use your information:**

    - We primarily use your information to improve your organization or the quality of its work, by delivering our key services: Research, Evaluation, Monitoring, Strategic Planning, UX research, Capacity Building, or “EBSS”.
    - Non-personal information is used for analytics, research, and to enhance the performance and security of our services.
    - Personal information is used to provide and improve our services, communicate with you, and fulfill your requests.
    - We may use your information to customize your experience with our services, including tailoring content and recommendations.

3. **Data and information security:**

    - We implement appropriate technical and organizational measures to safeguard your personal and organizational data against unauthorized access, disclosure, alteration, or destruction (*See section B: Information and Data Security Standards at EBD International*).
    - We regularly review and update our security practices to maintain the integrity and confidentiality of your data.

4. **Information sharing and disclosure:**

    - We do not sell, trade, or rent your personal information or organizational data to third parties.
    - If agreed (defined in contract), your information may be shared with trusted third-party service providers who assist us in delivering our services, provided they agree to maintain the confidentiality and security of your data.
    - We may disclose your information in response to legal obligations, to protect our rights or property, or to prevent illegal activities.

5. **Data retention:**

    - We retain your personal or organizational data for as long as necessary to fulfill the purposes outlined in this policy, unless a longer retention period is required or permitted by law.
    - Upon request, we will delete or anonymize your personal or organizational data in accordance with applicable laws and regulations.

6. **Your rights:**

    - You have the right to access, correct, or delete your personal information or organizational data. You may also request restrictions on the processing of your data or object to its processing under certain circumstances.
    - To exercise your rights or make inquiries about this Privacy, please contact us using the information provided below.

7. **Children's privacy:**

    - We do not knowingly collect personal information from children without parental consent.

8. **Compliance with GDPR:**

    - EBD International acknowledges and complies with the provisions of the General Data Protection Regulation (GDPR) regarding the processing of personal data of individuals within the European Economic Area (EEA). We ensure that your personal information is collected and processed lawfully, fairly, and transparently.
    - Where applicable, we will obtain your explicit consent before processing your personal data for specific purposes. You have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
    - We respect your rights under the GDPR, including but not limited to the right to access, rectify, erase, restrict processing, and data portability. You may exercise these rights by contacting us.
    - If you believe that we have not complied with the GDPR regarding your personal data, you have the right to lodge a complaint with the relevant supervisory authority.
    - EBD International is committed to upholding the principles and requirements of the GDPR to ensure the protection and privacy of your personal information.

9. **Changes to this policy:**

    - We reserve the right to update or modify Privacy & Information Security Policy at any time. We will notify you of any changes by posting the revised policy on our website or through other appropriate means.
    - In the event that you have a valid contract with EBD International at the time of changes to this policy, you will be notified of such changes in writing, via the

agreed communication channels. In that case, if you do not agree with the changes, you can decide that the changes made during the term of our contract do not apply to you. We are obliged to respect your decision.

10. Contact us:

- If you have any questions or concerns about our Privacy & Information Security Policy or the handling of your personal or organizational information, please contact us at info@ebdinternational.com

B: INFORMATION AND DATA SECURITY STANDARDS AT EBD INTERNATIONAL

Establish and maintain a comprehensive information security policy to ensure the confidentiality, integrity, and availability of data and systems.

---

1. ACCEPTABLE USE POLICY (AUP)

Purpose: Define acceptable conditions for using data, information and resources.

Applies to: All users accessing computing devices, data assets, and network resources.

Standards:

a) **Usage guidelines:**

- Employees must use company resources responsibly and ethically.
- Prohibited actions include unauthorized access, downloading malicious software, and inappropriate use of internet and email.

b) **Internet and Email use:**

- Internet and email services are for business purposes only.
- Prohibited actions include accessing offensive websites and sharing sensitive information via unsecured emails.

c) **Software Installation:**

- Only authorized personnel may install software on company devices.

d) **Remote Access:**

- Access to the company network from home requires secure methods such as VPN.

Implementation:

- Communicate the AUP to all employees.
- Conduct training sessions.
- Monitor compliance and enforce the policy.
- Review and update periodically.

---

2. NETWORK SECURITY POLICY (NSP)

Purpose: Outline principles, procedures, and guidelines to enforce, manage, monitor, and maintain data security on the corporate network.

Applies to: All users and networks.

Standards:

a) **Network Security Measures:**

- Implement firewalls, antivirus software, and intrusion detection systems.

b) **Access Control:**

- Restrict unauthorized access through secure login procedures and two-factor authentication.

c) **Monitoring:**

- Continuously monitor network traffic for suspicious activity.

d) **Incident Response:**

- Establish procedures for responding to network security incidents.

Implementation:

- Define and document the network architecture.
- Assign roles for network security management.
- Review and update the policy regularly.

---

3. DATA MANAGEMENT POLICY (DMP)

Purpose: Define measures for maintaining the confidentiality, integrity, and availability of data.

Applies to: All users and data storage and information processing systems.

Standards:

a) **Data inventory:**
   - Identify and classify data collected, processed, and stored.

b) **Access controls:**
   - Define access levels based on job roles.

c) **Data handling procedures:**
   - Establish procedures for data collection, processing, storage, and deletion.

d) **Compliance:**
   - Ensure compliance with data protection regulations (e.g., GDPR).

Implementation:

- Communicate the DMP to relevant stakeholders.
- Implement data protection tools and solutions.
- Review and update the policy regularly.

---

4. ACCESS CONTROL POLICY (ACP)

Purpose: Define the requirements for managing users' access to critical data and systems.

Applies to: All users and third parties with access to sensitive resources.

Standards:

a) **Access Levels:**
   - Create a hierarchy of user access permissions.

b) **Principle of Least Privilege:**
   - Grant users the minimum access necessary for their responsibilities.

c) **Authentication Methods:**
   - Implement two-factor authentication for critical systems.

d) **Regular Audits:**

- Conduct regular audits to review and adjust access permissions.

Implementation:

- Assign responsibilities for managing access controls.
- Communicate the ACP to all employees.
- Review and update the policy regularly.

---

5. PASSWORD MANAGEMENT POLICY (PMP)

Purpose: Outline requirements for securely handling user credentials.

Applies to: All users and third parties possessing credentials to organizational accounts.

Standards:

a) **Password Requirements:**
   - Define complexity, length, and rotation policies.

b) **Credential Management:**
   - Assign responsibilities for creating and managing passwords.

c) **Password Storage:**
   - Store passwords securely with AES 256-bit encryption.

d) **Password Management Tools:**
   - Implement tools for generating, delivering, and rotating passwords.

Implementation:

- Communicate the PMP to all employees.
- Conduct regular audits.
- Review and update the policy regularly.

---

6. REMOTE ACCESS POLICY (RAP)

Purpose: Define requirements for establishing secure remote access to data and systems.

Applies to: All users and devices accessing the infrastructure from outside the corporate network.

Standards:

a) **Remote Access Guidelines:**

- Establish secure remote access methods such as VPN.

b) **Device Security:**

- Ensure personal devices meet security standards.

c) **Monitoring:**

- Monitor and record remote user activities.

d) **Authentication:**

- Implement two-factor authentication for remote access.

Implementation:

- Communicate the RAP to all remote users.
- Conduct regular audits.
- Review and update the policy regularly.

---

7. VENDOR MANAGEMENT POLICY (VMP)

Purpose: Govern third-party risk management activities.

Applies to: All vendors, suppliers, partners, and third parties accessing corporate data and systems.

Standards:

a) **Vendor Assessment:**

- Conduct risk assessments of potential vendors.

b) **Compliance Checks:**

- Ensure vendors comply with cybersecurity requirements.

c) **Access Controls:**

- Implement access controls and monitoring for third-party access.

d) **Incident Management:**

- Establish procedures for managing third-party security incidents.

Implementation:

- Communicate the VMP to all relevant stakeholders.
- Conduct regular audits.
- Review and update the policy regularly.

---

8. REMOVABLE MEDIA POLICY

Purpose: Outline rules for using USB devices and measures for preventing USB-related security incidents.

Applies to: All users of removable media.

Standards:

a) **Usage Guidelines:**
   - Define acceptable use of USB devices.

b) **Device Management:**
   - Use software to monitor and control USB device connections.

c) **Whitelist/Blacklist:**
   - Create lists of allowed and prohibited devices.

d) **Incident Response:**
   - Establish procedures for responding to USB-related security incidents.

Implementation:

- Communicate the policy to all users.
- Conduct regular audits.
- Review and update the policy regularly.

---

9. INCIDENT RESPONSE POLICY

Purpose: Guide the response to data security incidents.

Applies to: Security officers, employees, information systems, and data.

Standards:

a) **Incident identification:**
   - Define types of incidents and detection methods.

b) **Roles and responsibilities:**
   - Assign roles for incident response.

c) **Response procedures:**

- Establish detailed response procedures for each type of incident.

d) **Communication strategies:**

- Define communication protocols during an incident.

e) **Post-Incident review:**

- Conduct post-incident reviews to improve response strategies.

Implementation:

- Communicate the policy to all relevant stakeholders.
- Conduct regular training sessions.
- Review and update the policy regularly.

---

10. SECURITY AWARENESS AND TRAINING POLICY

Purpose: Establish requirements for raising security awareness and conducting training.

Applies to: Security officers and staff organizing training sessions.

Standards:

a) **Training programs:**

- Develop and implement regular cybersecurity training sessions.

b) **Awareness campaigns:**

- Conduct awareness campaigns to highlight common threats and best practices.

c) **Simulated attacks:**

- Use simulations to evaluate and improve employees' response to cyber threats.

d) **Feedback and improvement:**

- Collect feedback from training sessions to improve future programs.

Implementation:

- Communicate the policy to all employees.
- Conduct regular training sessions.
- Review and update the policy regularly.

---

11. IMPLEMENTATION PROCESS FOR INFORMATION SECURITY POLICIES

a) **Assess the Risks:** Identify and evaluate information assets, potential threats, and vulnerabilities.

b) **Outline the Policy:** Create detailed policies based on risk assessment results.

c) **Implement the Policy:** Assign responsibilities, create compliance instructions, and implement security controls.

d) **Communicate the Policy:** Educate employees and stakeholders about the policies and their responsibilities.

e) **Monitor the Policy's Effectiveness:** Review logs, conduct audits, and update policies regularly to address new threats.

Adopted: November 30, 2022

Last update: April 8, 2023

Signed by

Srdjan Vujovic, EBD International CEO

Annex 1. Understanding of organizational data

An organization's data refers to all the information and data that it collects, generates, stores, and utilizes in the course of its operations. This data can be broadly categorized into several types:

1. **Operational data**:
    - **Transaction data**: Sales transactions, purchase orders, invoices, payment records.
    - **Production data**: Manufacturing processes, quality control records, inventory levels.
    - **Logistics data**: Shipping records, delivery schedules, transportation routes.
2. **Customer data**:
    - **Personal information**: Names, addresses, contact details.
    - **Behavioral data**: Purchase history, browsing behavior, customer feedback.
    - **Demographic data**: Age, gender, income level, education level.
3. **Financial Data**:
    - **Revenue and expenses**: Sales revenue, cost of goods sold, operating expenses.
    - **Financial statements**: Balance sheets, income statements, cash flow statements.
    - **Budgeting and forecasting**: Budget plans, financial projections, investment analysis.
4. **Employee Data**:
    - **Personal information**: Names, addresses, contact details, social security numbers.
    - **Work information**: Employment history, job roles, performance evaluations, salary details.
    - **Training and development**: Training programs attended, skills acquired, career development plans.
5. **Administrative data**:
    - **Policies and procedures**: Organizational policies, standard operating procedures.
    - **Compliance records**: Regulatory compliance documents, audit reports, certification records.
    - **Internal communications**: Meeting minutes, internal memos, emails.
6. **Market and competitive data**:
    - **Market research**: Industry reports, market analysis, customer surveys.

- **Competitive intelligence**: Information on competitors' products, pricing strategies, market positioning.

7. **Technical and product data**:
    - **Product specifications**: Design documents, technical specifications, user manuals.
    - **Research and development**: Research papers, experimental data, patent information.
    - **IT Data**: System logs, software configurations, network diagrams.
8. **Legal and compliance data**:
    - **Contracts and agreements**: Legal contracts, partnership agreements, NDAs.
    - **Regulatory documents**: Licenses, permits, compliance certificates.
9. **Strategic data**:
    - **Strategic plans**: Strategic plans, business models, growth and development strategies, operative plans, and related reports.
    - **Performance metrics**: Key performance indicators (KPIs), benchmarking data.
10. **Other data**

Annex 2: Privacy & Information Security Policy Acknowledgment Form

Employee/Consultant Information:

- Name: _____
- Position/Role: _____
- Date: _____

Acknowledgment:

I, _____ (print name), acknowledge that I have received, read, and understood the Privacy & Information Security Policy of EBD International. I understand the importance of this policy and my role in ensuring the protection of sensitive information and the security of data.

I agree to comply with all the guidelines, standards, and procedures outlined in the policy. I am aware that any breach of this policy may result in disciplinary action, including termination of employment or contract, and/or legal action.

I understand that it is my responsibility to stay informed about any updates or changes to the policy and to participate in any required training sessions related to information security.

I hereby certify that I will uphold the principles and requirements set forth in the Privacy & Information Security Policy to the best of my ability.

Signature (Employee/Consultant Signature): _____

For Internal Use Only:

Received by: _____
Position: _____
Date: _____