



CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate.**
- **Restore normal operations and services.**

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

- Formal and effective policies and procedures governing all the following:
 1. Data governance and classification.
 2. Access controls and identity management.
 3. Business continuity and disaster recovery.
 4. Configuration management.
 5. Asset management.
 6. Risk assessment.
 7. Data disposal.
 8. Incident response.
 9. Systems operations.
 10. Vulnerability and patch management.
 11. System, application and network security and monitoring.
 12. Systems and application development and performance.
 13. Physical security and environmental controls.
 14. Data privacy.
 15. Vendor and third party service provider management.
 16. Consistent use of multi-factor authentication.
 17. Cybersecurity awareness training, which is given to all personnel annually.
 18. Encryption to protect all sensitive information transmitted and at rest.

2. Prudent Annual Risk Assessments.

A Risk Assessment is an effort to identify, estimate, and prioritize information system risks. IT threats are constantly changing, so it is important to design a manageable, effective risk assessment schedule. Organizations should codify the risk assessment's scope, methodology, and frequency. A risk assessment should:

- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized.
- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks.
- Describe how the cybersecurity program will mitigate or accept the risks identified.
- Facilitate the revision of controls resulting from changes in technology and emerging threats.
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

3. A Reliable Annual Third Party Audit of Security Controls.

Having an independent auditor assess an organization's security controls provides a clear, unbiased report of existing risks, vulnerabilities, and weaknesses.

As part of its review of an effective audit program, EBSA would expect to see:

- Audit reports, audit files, penetration test reports and supporting documents, and any other analyses or review of the party's cybersecurity practices by a third party.
- Audits and audit reports prepared and conducted in accordance with appropriate standards.
- Documented corrections of any weaknesses identified in the independent third party analyses.

4. Clearly Defined and Assigned Information Security Roles and Responsibilities.

For a cybersecurity program to be effective, it must be managed at the senior executive level and executed by qualified personnel. As a senior executive, the Chief Information Security Officer (CISO) would generally establish and maintain the vision, strategy, and operation of the cybersecurity program which is performed by qualified personnel who should meet the following criteria:

- Sufficient experience and necessary certifications.
- Initial and periodic background checks.
- Regular updates and training to address current cybersecurity risks.
- Current knowledge of changing cybersecurity threats and countermeasures.

5. Strong Access Control Procedures.

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to IT systems and data. It mainly consists of two components: authentication and authorization. The following are best security practices for access control:

- Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.
- Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.
- Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.
- All employees use unique, complex passwords.
- Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.
- Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with, nonpublic information.
- Procedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant.
- Confirm the identity of the authorized recipient of the funds.

6. Assets or Data Stored in a Cloud or Managed by a Third Party Service Provider are Subject to Appropriate Security Reviews and Independent Security Assessments.

Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. Organizations must understand the security posture of the cloud service provider in order to make sound decisions on using the service.

Best practices include:

- Requiring a risk assessment of third party service providers.
- Defining minimum cybersecurity practices for third party service providers.
- Periodically assessing third party service providers based on potential risks.

- Ensuring that guidelines and contractual protections at minimum address the following:
 - » The third party service provider's access control policies and procedures including the use of multi-factor authentication.
 - » The third party service provider's encryption policies and procedures.
 - » The third party service provider's notification protocol for a cybersecurity event which directly impacts a customer's information system(s) or nonpublic information.

7. Cybersecurity Awareness Training Conducted at Least Annually for All Personnel and Updated to Reflect Risks Identified by the Most Recent Risk Assessment.

Employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat. Since identity theft is a leading cause of fraudulent distributions, it should be considered a key topic of training, which should focus on current trends to exploit unauthorized access to systems. Be on the lookout for individuals falsely posing as authorized plan officials, fiduciaries, participants or beneficiaries.

8. Secure System Development Life Cycle Program (SDLC).

A secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort. Best practices include:

- Procedures, guidelines, and standards which ensure any in-house applications are developed securely. This would include such protections as:
 - » Configuring system alerts to trigger when an individual's account information has been changed.
 - » Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account.
 - » Requiring additional validation for distributions (other than a rollover) of the entire balance of the participant's account.
- Procedures for evaluating or testing the security of externally developed applications including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests, particularly with respect to customer-facing applications.

9. A Business Resiliency Program which Effectively Addresses Business Continuity, Disaster Recover, and Incident Response.

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. The core components of a program include the Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan.

- The Business Continuity Plan is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption.
- The Disaster Recovery Plan is the documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption.
- The Incident Response Plan is a set of instructions to help IT staff detect, respond to, and recover from security incidents.

An effective Business Resiliency Program should:

- Reasonably define the internal processes for responding to a cybersecurity event or disaster.
- Reasonably define plan goals.
- Define the documentation and reporting requirements regarding cybersecurity events and responses.
- Clearly define and describe the roles, responsibilities, and authority levels.
- Describe external and internal communications and information sharing, including protocols to notify plan sponsor and affected user(s) if needed.
- Identify remediation plans for any identified weaknesses in information systems.
- Include after action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
- Be annually tested based on possible risk scenarios.

10. Encryption of Sensitive Data Stored and in Transit.

Data encryption can protect nonpublic information. A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.

11. Strong Technical Controls Implementing Best Security Practices.

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Best security practices for technical security include:

- Hardware, software and firmware models and versions that are kept up to date.
- Vendor-supported firewalls, intrusion detection and prevention appliances/tools.
- Current and regularly updated antivirus software.
- Routine patch management (preferably automated).
- Network segregation.
- System hardening.
- Routine data backup (preferably automated).

12. Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its participants, including:

- Informing law enforcement.
- Notifying the appropriate insurer.
- Investigating the incident.
- Giving affected plans and participants the information necessary to prevent/reduce injury.
- Honoring any contractual or legal obligations with respect to the breach, including complying with agreed upon notification requirements.
- Fixing the problems that caused the breach to prevent its recurrence.

