Security Measures

Presented by:	**ADP - Global Security Organization**
Version:	**2.0**
Released:	**September 2019**

Contents

Terms and Definitions

The following terms may appear throughout the document:

Term or Acronym used	Definition
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Overview

ADP maintains a formal information security program containing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of client information. This program is reasonably designed to (i) safeguard the security and confidentiality of client information, (ii) protect against anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information.

This document contains an overview of ADP's information security measures and practices, as of the release date and which are subject to change by ADP. These requirements and practices are designed to be consistent with the ISO/IEC 27001:2013 information security standards. ADP periodically assesses its security policies and standards. Our goal is to help ensure that the security program effectively and efficiently operates to protect all the information entrusted to us by our clients and their employees.

.

Section 1 - Information Security Policies

Independence of Information Security Function

ADP's Chief Security Officer oversees ADP's Global Security Organization (GSO) and reports to the General Counsel (GC), instead of to the Chief Information Officer, which gives GSO the necessary independence from IT. The GSO is a cross-divisional, converged security team that has a multi-disciplinary approach in cyber and information security and compliance, operational risk management, client security management, workforce protection, and business resilience. GSO senior management, under our Chief Security Officer, are responsible for managing security policies, procedures, and guidelines.

Formal Definition of an Information Security Policy

ADP has developed and documented formal information security policies that set out ADP's approach to managing information security. Specific areas covered by this policy include, but are not limited to:

- **Security Management Policy –** Outlines the responsibilities of the Global Security Organization (GSO) and the Chief Security Officer (CSO), including the information security responsibilities and controls on hiring process from a security perspective.
- **Global Privacy Policy -** Discusses the collection of personal information, access to, accuracy, disclosures, and privacy statement to clients.
- **Employees Acceptable Use of Electronic Communications and Data Protection Policy** – Describes acceptable use, different electronic communications, encryption, and key management.
- **Information Handling Policy –** Provides requirements for the classification of ADP information and establishes protection controls.
- **Physical Security Policy–** Defines the security requirements of ADP facilities and subsequently our employees and visitors who work there.
- **Security Operations Management Policy –** Provides minimum controls for maintaining system patches, effectively addresses the threat from malware, and maintains backups and database security controls.
- **Security Monitoring Policy –** Provides controls for intrusion detection systems (IDS), logs, and data loss prevention (DLP).
- **Investigations and Incident Management Policy –** Defines standards for incident response, electronic discovery, workforce protection, and access to employees electronic stored information.
- **Access & Authentication Policy –** Outlines requirements for authentication (e.g. user ID and password), remote access, and wireless access.
- **Network Security Policy –** Security architecture of routers, firewalls, AD, DNS, email servers, DMZ, cloud services, network devices, web proxy, and switched network technology.
- **Global Third-Party Risk and M&A Policy –** Defines minimum security controls for engaging any third party to assist ADP in achieving its business objectives.
- **Application Management Policy –** Establishes appropriate security controls into each stage of the system development lifecycle.
- **Business Resiliency Policy –**Governs the protection, integrity and preservation of ADP by establishing the minimum requirements to document, implement, maintain, and continually improve Business Resiliency Programs
- **Converged Security Risk Management Policy –** Identification, monitoring, response, analysis, governance, and new business initiatives.

Policies are published in the ADP intranet and are accessible to all employees and contractors from within the ADP network.

Information Security Policy Review

ADP reviews its information security policies at least once per year or whenever there are major changes impacting the functioning of ADP's information systems.

Section 2 - Organization of Information Security

Information Security Roles and Responsibilities

The GSO consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined for all members of the GSO. The GSO is charged with the design, implementation and oversight of our information security program based on corporate policies. The GSO's activities are overseen by the Executive Security Committee, whose members include ADP's Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer, and General Counsel.

Mobile Computing and Teleworking Policy

ADP requires all confidential information to be encrypted on mobile devices, to prevent data leakage, which could result from theft or loss of a computer / device. Advanced end-point protection and two-factor authentication over VPN is also required to access the corporate networks remotely. All remote devices are required to be password protected. ADP employees are required to report lost or stolen remote computing devices immediately through a Security Incident Reporting Process.

All employees and contractors, as a condition of employment with ADP, must comply with the Acceptable Use of Electronic Communications and Data Protection Policy and other relevant policies.

Section 3 - Human Resource Security

Background Checks

Consistent with applicable legal requirements in the individual's jurisdiction, ADP conducts appropriate background checks commensurate with the duties and responsibilities of its employees, contractors and third parties. These checks confirm the candidate's suitability for handling clients' information prior to engaging or hiring such individuals.

Background screening may include the following components:

- Identity/employment eligibility verification
- Employment history
- Educational history and professional qualifications
- Criminal records (where legally authorized and depending on local country regulations)

Confidentiality Agreements with Employees and Contractors

ADP employment contracts and contracts with contractors contain terms that indicate obligations and responsibilities related to client information to which they will have access. All ADP employees and contractors are bound by confidentiality obligations.

Information Security Training Program

All employees are required to complete information security training as part of their onboarding plan. In addition, ADP delivers annual security training to remind employees of their responsibilities when performing their day-to-day duties.

Employees' Responsibilities and Disciplinary Processes

ADP has published a security policy that all ADP employees must comply with. Violations of security policies may lead to revocation of access privileges and/or disciplinary actions up to and including termination of consulting contracts or employment.

Termination of Employment Responsibilities

Responsibilities upon termination of employment have been formally documented and include, at minimum:

- Return all ADP information and assets in the possession of the respective employee, on whatever medium it is stored
- Termination of access rights to ADP facilities, information and systems
- Change of passwords for remaining active shared accounts, if applicable
- Transfer of knowledge, if applicable.

Section 4 - Asset Management

Acceptable Use of Assets

Acceptable use of assets is explained in several policies, applicable to ADP employees and contractors, to help ensure that ADP's and clients' information are not exposed by use of such assets. Examples of areas described in these policies are: use of electronic communications, use of electronic equipment, and use of information assets.

Classification of Information

Information acquired, created or maintained by or on behalf of ADP is assigned, as applicable, a security classification of:

- Public- Example: Marketing brochures, published annual reports
- ADP Internal Use Only- Example: Interoffice communications, operating procedures
- ADP Confidential- Example: Personal and Sensitive Personal Information
- ADP Restricted- Example: Financial forecasts, strategic planning information

Requirements for handling information are directly correlated to the information security classification. Personal Information and Sensitive Personal Information are always considered ADP Confidential. All client information is classified as confidential.

ADP employees are accountable for protecting and handling information assets in accordance with their security classification level, which provides protection of information and applicable handling requirements for each classification level. The ADP confidentiality classification is applied to all information stored, transmitted, or handled by third parties.

Equipment and Media Disposal

When ADP equipment, documents, files, and media are disposed of or reused, appropriate measures are taken to prevent subsequent retrieval of client's information originally stored in them. All information on computers or electronic storage media, regardless of classification, is securely disposed of, unless the media is physically destroyed, before being released outside ADP facilities or repurposed. The procedures for the secure destruction/erasure of ADP information held on equipment, in documents, files, and media are formally documented.

Physical Media in Transit

Organizational safeguards have been implemented to protect printed materials containing clients' information against theft, loss, and/or unauthorized access/modification (i) during transit e.g. sealed envelopes, containers and hand delivery to authorized user; and (ii) during review, revision or other processing where removed from secure storage.

Section 5 - Access Control

Business Requirements of Access Control

ADP's Access Control Policy is based on business-defined requirements. The policies and control standards are articulated into access controls that are enforced in all components of the provided service and are based on a "least-privilege" and "need to know" principle.

Access to Infrastructure - Access Control Management

Access requests to move, add, create, and delete are logged, approved and periodically reviewed.

A formal review is performed, at least yearly, to confirm that individual users accurately correspond to the relevant business role and would not have continued access after a position change. This process is audited and documented in a SOC1[1] type II report. From within an Identity Management System, a dedicated ADP team is responsible for granting, denying, cancelling, terminating and decommissioning/deactivating access to ADP facilities and information systems. ADP uses a centralized identity and access management (IAM) tool that is managed centrally by a dedicated GETS team. According to the access rights requested through the centralized IAM tool, a validation workflow will be triggered that could involve the users' supervisor. Access is provided on a temporary basis and workflows exist to prevent such access from remaining permanent. An employee's access to a facility is decommissioned immediately after the last day of employment by deactivating their access card (employee badge). The employee's user IDs are immediately deactivated. All employee's assets are returned and checked by the competent line manager and are compared against the asset list in the configuration management data base. Following a job position change, or organizational changes, user profiles or user access rights are required to be modified by the applicable business unit management and the IAM Team. Additionally, a formal review of access rights is performed every year to verify that individual users' rights correspond to their relevant business role and that there are no remaining irrelevant access rights after a position transfer.

Password Policy

ADP associate password policies are enforced in servers, databases and network devices and applications, to the extent the device/application allows it. The password complexity is derived from a risk-based analysis of the protected data and content. The policies meet prevailing industry standards for strength and complexity, including but not limited to the use of step-up, two-factor, or biometric authentication where appropriate.

Client application authentication requirements vary by product, and federated services (SAML 2.0) are available on specific ADP applications using a unified network and security layer managed by GETS.

Session Timeouts

ADP enforces automatic timeouts to all servers, workstations, applications and VPN connections based upon a risk-based approach consistent with industry standards. Re-establishment of sessions may take place only after the user has provided a valid password.

[1] In the case of certain US Services offered by ADP, this is audited in a SOC 2 Type 2 report.

Section 6 - Cryptography

Cryptographic Controls

ADP requires that sensitive information exchanged between ADP and ADP third parties must be encrypted (or transport channel must be encrypted) using industry accepted encryption techniques and strengths. Alternatively, a private leased line may be used.

Key Management

ADP has an internal Encryption Security Standard that includes well-defined key management and key escrow procedures, including both symmetric and asymmetric keys management.

Encryption keys used for ADP information are always classified as confidential information. Access to such keys is strictly limited to those who have a need to know and, if an exception approval is provided. Encryption keys and key lifecycle management followed industry standard practices.

Section 7 - Physical and Environmental Security

ADP's approach to physical security has two objectives – creating a safe work environment for ADP associates and protecting Personal Information held in ADP data centers and other strategic ADP locations.

ADP security policy requires ADP management to identify those areas requiring a specific level of physical security. Access to those areas is provided only to authorized associates for authorized purposes. ADP secured areas employ various physical security safeguards, including video surveillance systems, use of security badges (identity-controlled access) and security guards stationed at entry and exit points. Visitors may only be provided access where authorized and are supervised at all times.

Section 8 - Operations Security

Formalization of IT Operations Procedures

GETS is the ADP unit responsible for IT infrastructure operations and maintenance. GETS formally maintains and documents IT operations policies and procedures. These procedures include, but are not limited to the following:

- Change management
- Back-up management
- System error handling
- System restart and recovery
- System monitoring
- Jobs scheduling and monitoring

Infrastructure Change Management

A periodic Change Advisory Board (CAB), including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings discuss impacts deployment windows and promotions to production, as well as to coordinate any other change in the production infrastructure.

System Capacity Planning and Acceptance

Capacity requirements are continuously monitored and regularly reviewed. Following these reviews, systems and networks are scaled up or down accordingly. When significant changes must be made due to a change in capacity or a technological evolution, the GETS benchmarking team may perform stress tests to the relevant application and/or system. At the conclusion of stress testing, the team provides a detailed report of performance evolution by gauging the changes in (i) components, (ii) system configuration or version, or (iii) middleware configuration or version.

Protection Against Malicious Code

Industry standard endpoint protection technologies are leveraged to protect ADP assets in accordance with industry standard best practices.

Back-Up Management Policy

ADP has policies in place that require all production hosting operations to back-up production information. The scope and the frequency of back-ups are executed in accordance with the business requirements of relevant ADP services, the security requirements of the information involved, and the criticality of the information with respect to disaster recovery. Monitoring of scheduled back-ups is performed by GETS, to identify back-up issues or exceptions.

Security Logging and Monitoring

ADP has implemented a central and read-only logging infrastructure (SIEM) and a log correlation and alerting system (TPSI). Log alerts are monitored and treated in a timely manner by the CIRC.

All of these systems are synchronized using a unique Network Time Protocol (NTP)based clock reference.

Each individual log contains, at minimum:

- Timestamp
- Who (identity of the operator or administrator)
- What (information about the event)

Audit trails and system logging for ADP applications are designed and set up to track the following information:

- Authorized access
- Privileged operations
- Unauthorized access attempts
- Systems alerts or failures
- Changes to systems security settings, when the system allows such logging

These logs are only available to ADP authorized personnel and are sent in live mode to prevent data from being tampered with before being stored in the secure logging appliances.

Infrastructure Systems and Monitoring

ADP uses appropriate measures to provide infrastructure monitoring 24 hours per day, 7 days per week. Disruption alerts are managed by different teams according to their severity level and the skills required to resolve them.

ADP hosting center facilities employ monitoring applications that are constantly running on all related processing systems and on the network components to provide ADP staff proactive notification of issues and warnings in anticipation of possible problems.

Technical Vulnerability Management

All computers installed in the hosting infrastructure must comply with the installation of a specialized security hardened operating system (or secure build process). Hosted operations employ a hardened, approved, and standardized build for every type of server used within our infrastructure. Out-of-the-box installation of operating systems is prohibited since these installations may create vulnerabilities, such as generic system account passwords, that would introduce an infrastructure risk. These configurations reduce the exposure of hosted computers running unnecessary services that can lead to vulnerabilities.

ADP has a documented methodology for conducting release and periodic vulnerability assessments and compliance reviews of Internet facing web-based applications and their corresponding infrastructure components, which include at least 15 primary categories of testing. Assessment methodology is based on both internal and industry best practices, including, but not limited to, Open Web Application Security Project (OWASP), SANS Institute and Web Application Security Consortium (WASC).

Section 9- Communications Security

Network Security Management

ADP employs a network-based intrusion detection system that monitors traffic at the network infrastructure level (24 hours a day, 7 days a week) and identifies suspicious activity or potential attacks.

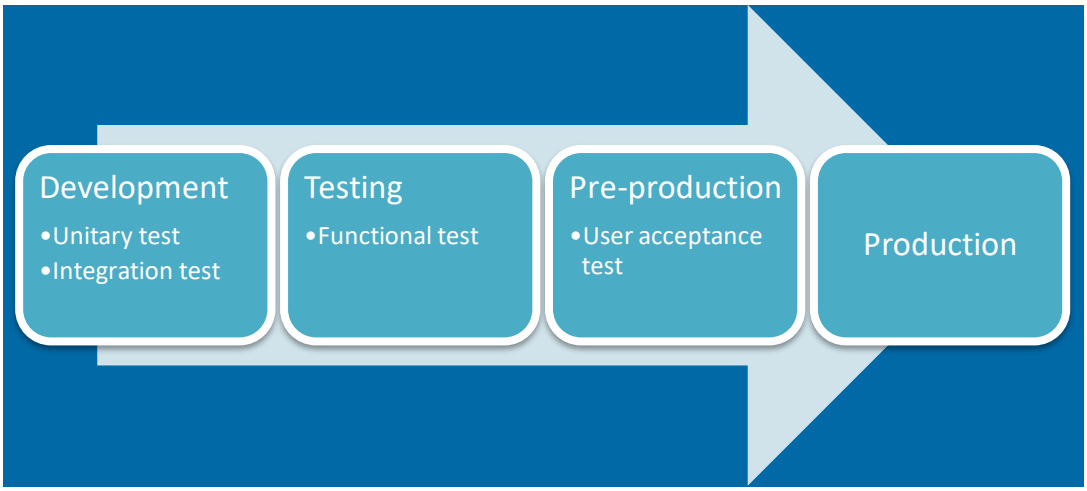
Exchange of Information

ADP implements appropriate controls so that ADP clients' information sent to third parties is transferred between authorized information systems and resources only and is only exchanged through ADP’s secure and authorized transfer mechanisms.

Section 10 - System Acquisition, Development, and Maintenance

Security in Development and Support Processes

During the development cycle, applicable documentation is generated, and testing plans are built for the testing phase. Different stages are defined for each environment with relevant approval at each phase:



- To move from Testing to Pre-production environment, approval from ADP's Quality team is required.
- To move from Pre-production to Production, approval from IT Operations is required.

Development teams are required to utilize secure coding methods. Application changes are tested in development and regression environments before they reach the production systems. Tests are performed and documented. Upon approval, changes are deployed into production. Penetration testing is performed after significant changes.

A periodic CAB, including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings take place on a regular basis, and are meant to discuss impacts, to agree on deployment windows and to approve the promotion of software packages to production, as well as to inform about any other changes in production infrastructure.

ADP's IT Operations team provides the final approval before promotion to production environment of the software packages.

Security in Development Environment

Production and development environments are segregated and independent from each other. Appropriate access controls are employed to enforce proper segregation of duties. Software packages are accessible at each stage of the development process and only by the teams involved in that stage.

Test Data

Per ADP's Application Management Policy, the use of real or un-sanitized data in development and testing is not permitted unless explicitly requested and authorized by client.

Section 11 - Supplier Relationships

Identification of Risks Related to External Parties

Risk assessments of third parties who require access to ADP and/or client information are periodically performed to determine their compliance with ADP security requirements for third parties, and to identify any gaps in the applied controls. If a security gap is identified, new controls are agreed upon with such external parties.

Information Security Agreements with External Parties

ADP enters into agreements with all third parties which include appropriate security commitments to meet ADP's security requirements.

Section 12 - Information Security Incident Management

Management of Information Security Incidents and Improvements

ADP has a documented methodology for responding to security incidents timely, consistently, and effectively.

Should an incident occur, a predefined team of ADP employees activates a formal incident response plan that addresses areas such as:

- Escalations based on the classification of incident or incident severity
- Contact list for incident reporting/escalation
- Guidelines for initial responses and follow up with involved clients
- Compliance with applicable security breach notification laws
- Investigation log
- System recovery
- Issue resolution, reporting, and review
- Root Cause and Remediation
- Lessons learned

ADP policies define a security incident, incident management, and all employees' responsibilities regarding the reporting of security incidents. ADP also conducts regular training for ADP employees and contractors to help ensure awareness of reporting requirements. Training is tracked to ensure completion.

Section 13- Information Security Aspects of Business Resiliency Management

ADP Business Resiliency Program

ADP is committed to keeping our services and operations running smoothly, so that we can provide our clients with the best service possible. It's our priority to identify — and mitigate — the technology, environmental, process, and health risks that may get in the way of providing our business services. ADP has created an integrated framework that lays out our mitigation, preparedness, response, and recovery processes and includes:

- Risk Assessment
- Risk Threat Analysis
- Business Impact Analysis
- Plan Development
- Business Continuity Planning
- Disaster Recovery Planning
- Health and Safety Planning
- Real-World Response
- Crisis Management
- Emergency Response
- Testing and Validation
- Review
- Revise
- Exercise

Section 14- Compliance

Compliance with Security Policies and Standards

ADP employs a process to internally perform compliance reviews on a periodic basis. Additionally, ADP performs a SOC1[2] type II audit on a periodic basis. These audits are conducted by a well-known third-party audit firm and audit reports are available on a yearly basis for clients upon request, when applicable.

Technical Compliance

To enforce technical compliance with best practices, ADP performs regularly scheduled network vulnerability scans. The scan results are then prioritized and developed into corrective action plans with the hosting teams and their management.

Vulnerability scans are performed on a regular basis of both internal and external environments. Additionally, source code scans and penetration testing are performed on a product-by-product basis. Utilizing specialized application scanning tools, application level vulnerabilities, if any, are identified, shared with the product development management teams, and incorporated into the quality assurance processes for corrective action. The results are analyzed, and corrective action plans developed and prioritized.

Retention of Data

ADP's data retention policy regarding client information is designed to comply with applicable laws. At the end of a client contract, ADP complies with its contractual obligations related to the client's information. ADP will return or allow the client to retrieve (by data download), all client information required for the continuity of the client's business activities (if not previously provided). Then, ADP will securely destroy remaining client information, except to the extent required under applicable law, authorized by the client or needed for dispute resolution purposes.

[2] In the case of certain US Services offered by ADP, there would be also SOC 2 Type II exec. reports