INFORMATION SECURITY RESPONSIBILITIES SUMMARY

A more human resource.®

Scope
This Summary applies to individuals who provide services to ADP on a provisional or non-permanent basis, such as temporary workers, contract workers, independent contractors, or consultants worldwide ("Contingent Workers").

Purpose
This Summary sets forth the fundamental principles all Contingent Workers must adhere to in order to insure the protection of ADP associate data, Contingent Worker data, as well as ADP client data. ADP has an ethical and legal obligation to safeguard client, associate and company information, as well as to protect the privacy of individuals whose data we maintain. All Contingent Workers engaged with ADP are responsible for adhering to all ADP policies and standards as outlined in this document, subject to the requirement of local law.

Protecting Information – All client data, and much of ADP's internal data, is considered ADP Confidential. All Contingent Workers have a responsibility to protect this information when viewing, storing, using, transmitting, or disposing it. Protection is required regardless of how it is stored. Your responsibilities specifically include, but are not limited to, the following:

1. Never access or view information classified as ADP Confidential (example: client data) without a valid business reason.

2. Protect client information and other classified information, like Sensitive Personal Information by following the guideline below:
    - Encourage clients to pull their own reports and/or access their own information, from within their application/system.
    - Do not send Sensitive Personal Information via email, outside of ADP's network, even if it is encrypted.
    - Provide access to classified information on a need-to-know basis.
    - Do not provide classified information to a third party without the written authorization of the client or permission from the Legal department.
    - Do not provide classified information to anyone unless you are sure of the identity and authority of that person.
    - Be on the lookout for potential scams or social engineering efforts, which request information about you, ADP, or our associates or clients.

3. Never use Sensitive Personal Information or other production data (example, client data) for development, testing, training, presentations or any purpose other than providing production service, client-specific acceptance testing, or production diagnostics.
    - Client data may be stored in various forms, including but not limited to:
        - Hard copy
        - Electronic
        - Voice recordings
    - Do not copy client data from production to test environments. If this is required for business purposes, the data must be de-identified to ensure data cannot be traced to a client or client employee.

- Any situation that requires the use of client data for development or testing, unrelated to that specific client, must go through the GSO Operational Risk Management process.

4. Classify, label and handle information appropriately. The classifications are:
   - ADP Internal Use Only
   - ADP Confidential
   - ADP Restricted

5. Use only secure methods to communicate or transmit classified information.
   - Keep conference calls and video conferences secure by requiring access codes
   - Secure physical information presented in meetings/conferences.
   - Be cautious of discussing classified information in public areas.
   - Secure transmissions include, but are not limited to: secure email, secure file transfer and encrypted electronic media.
   - Always confirm that the recipient list is correct before sending an email.
   - Under no circumstances should you send classified information outside of ADP without using a secure method.
   - If you are unsure as to what tools or methods exist that will allow you to securely transmit classified information please contact your Business Security Officer.

Securing Your Workstation and Computer – Protect the information entrusted to you by securing your workspace and computer.

6. ADP issued laptops, cellular phones and other mobile devices are often stolen or lost. These devices must remain in your possession at all times or be secured in a locked office or cabinet if you leave them unattended.
   - To prevent theft, always maintain physical possession of your mobile device when traveling (example, don't leave it in a hotel room or car.)
   - If you are unable to maintain physical possession, then lock your mobile device in the trunk of the car. The mobile device should also be powered off.
   - Never leave your laptop overnight in a vehicle.
   - Do not check a laptop or mobile device as baggage on any form of transportation or leave it in a hotel luggage storage area.
   - Do not keep passwords, access cards, key fobs/tokens, or hard copy classified information with your laptop.
   - Do not share your passwords or access credentials with anyone.
   - Only authorized ADP personnel can provide maintenance/support for ADP issued equipment.

7. Every time you leave your workspace, lock your computer. If you need assistance, please contact your local computer support.

8. Practice safe computing.
   - Do not click on an imbedded link in a suspicious email.
   - Do not open a file attached to suspicious email.

- Be very suspicious of emails seeking your credentials or classified information.

9. Keep a Clean Desk
   - At the end of each work day or shift, and during absences from your work area (including work areas at home and other non-ADP locations), secure classified information, both electronic and hard copy
   - Keep classified data for only as long as it is needed.

10. Use only approved document disposal services or shred all hardcopy documents containing classified information when you are finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair, or preparing to reuse electronic media such as CD, magnetic tape, hard drive, USB flash drive and other mobile devices.

11. Only ADP workstations and mobile devices may be used for ADP business purposes. They must be imaged, controlled and supported by ADP. This includes those devices remotely connected to an ADP network via VPN.

Maintaining Physical Security – Safeguard access to ADP facilities.

12. Openly display your ADP identification badge at all times when in ADP facilities.

13. Report any person not displaying a badge to your supervisor or nearest security staff member.

14. Make sure others do not “tailgate” into a facility behind you, and that your guests and vendors sign in with building security or reception, obtain and wear visitor passes, and are accompanied at all times.

15. If you misplace or lose your badge, report it immediately.

Learn About Security – Stay aware, informed and alert in order to maintain security. Threats and technology are constantly changing.

16. ADP offers various forms of security awareness and training. Stay current by taking full advantage of this training.

Report Security Incidents and Violations – Promptly report all security incidents, violations and suspicious activity so that they may be properly addressed.

17. Security incidents must be promptly reported. A security incident includes any compromise of classified information that results in the accidental or intentional exposure of ADP or client information to an unauthorized party as well as events that compromise ADP facilities, resources or systems.

18. Contact your facility security department or on-site management immediately if you notice suspicious visitors or activity.

19. To report fraud, workplace violence or threats, contact the GSO at 001-800-869-7687, or email Investigations@adp.com.

Protecting Computer Hardware and Software

20. Associates and Contingent Workers are only permitted to install ADP standard hardware and software. Installing non-standard hardware and software may violate copyright laws and security policy.

Acceptable Use of Electronic Communications – Electronic communications are an effective and common means of communication for both business and non-business use.

21. The use of ADP electronic communication systems, such as email and internet access, is acceptable for non-business purposes if the level of use is occasional, does not interfere with professional responsibilities, does not diminish productivity, does not lead to the degradation or disruption of the normal service levels, and does not violate any law or ADP policy.

22. Business communications must be made through ADP systems, therefore personal email accounts must not be used for ADP business purposes.

Disciplinary Action – Failure to follow this policy may result in termination of employment, subject to applicable local law. Requests to deviate from any security policy must go through the respective Business Security Officer for your BU or country.

Remember: You are responsible for protecting the information that is entrusted to you. If you are not sure about how to comply with any of these requirements, or if you become aware of violations of ADP security policies, please check with your manager or Business Security Officers. You may also call the ADP Ethics Hotline at 001-800-273-8442

Definitions:

De-identified	Full and complete irreversible user de-identification, or sanitization, via an accepted and approved data anonymization or de-identification method is required and MUST be performed on ANY source user data copied outside of the production environments for development or testing purposes.
Information Classifications	ADP information and client information entrusted to ADP must be classified and protected in a manner commensurate with its sensitivity. This is required no matter where it resides, what technology is used to process or store it, or the purpose for which it is used. ADP associates are responsible for protecting confidential ADP and client information from unauthorized access, modification, duplication, destruction or disclosure, whether accidental or intentional. The classification levels used by ADP are: • Public • ADP Internal Use Only • ADP Confidential

	• ADP Restricted Newly created, revised, or previously unmarked documents, which do not have one of the above classification labels, and is not used for advertising or marketing, will be classified as ADP Confidential by default.
Public	is information which is within the public domain and can be shared with anyone inside or outside of ADP. The dissemination of Public Information would not expose ADP to financial loss, embarrassment or jeopardize the security of ADP assets. Appropriate copyright laws and labeling (where appropriate) must be followed. Examples of public information include: • Marketing brochures • Published annual reports • Interviews with news media • Business cards • Press releases
ADP Internal Use Only	information is typically required to perform normal day-to-day work and may be accessed by ADP associates. Internal Use Only information may be shared within ADP, but should not be shared with consultants, vendors or temporary workers unless a non-disclosure agreement has been signed. Applicable ADP standards relating to the handling, access, use, disposal must be followed. Information should be classified as Internal Use Only if it includes at least one of the following characteristics and is not classified as Restricted or Confidential: • Commonly shared (internal) information, including operating procedures, policies and interoffice memorandums • Internal telephone directories • Information identifying a client, but excluding any financial data such as balances, safekeeping positions, credit data, etc. • Source Code (example: scripts used to perform some internal automation)
ADP Confidential	is information whose unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on ADP, its associates or clients. ADP Confidential information represents most information created or used within ADP, including most documents and email. ADP Confidential information includes information used in the provision of products and services to clients and prospective clients of ADP. Confidential information may be shared with parties who have a relationship with ADP, if they have signed a non-disclosure agreement, have been granted proper authorization and have a need to know. Applicable ADP standards relating to the handling, access, use, disposal must be followed. Confidential Information includes, but is not limited to: • Personal Information (defined below) • Sensitive Personal Information (defined below) • Information regarding clients and associates, including payroll information, that ADP is obligated to protect. • Information classified as “production”, including all client information when used in system testing or development environments. • Client or prospective client information supplied for the provision of ADP products and services or business requirements, and other proprietary system design, development or testing documentation. • Internal and external audit reports

	• Regulatory agency reports, unless specified by the regulatory agency as Public information
	• Information which an Information Owner / Information Steward determines has the potential for providing a competitive advantage
	• Information which an Information Owner / Information Steward determines is confidential to ADP.
	• Voice mail access codes and passwords
	• Passwords
	• Any form of security key
	  ○ Personal identification numbers
	  ○ One time registration codes
	  ○ Challenge/response phrases
	• Source Code (example: an application that enhances client sales and retention.)

Personal Information	is a subset of ADP Confidential Information and may require additional protections as a matter of law and/or relevant ADP policies and standards. Personal Information is information which (alone or when used in combination with other information within ADP's direct control) can be used to identify, locate or contact an individual, together with information related to such individual. Personal Information includes all Sensitive Personal Information and other obvious information, such as person's name or email address, as well as less obvious information such as any Internet Protocol address or biometric data, if such data could possibly be associated with an individual. Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files.

Sensitive Personal Information	is a subset of Personal Information, which due to its nature has been classified by law or by policy as deserving additional privacy and security protections. Sensitive Personal Information includes the following types of data:
	• All Government issued identification numbers, such as:
	  ○ U.S. Social Security Numbers
	  ○ Canada's Social Insurance Number or similar numbers in other countries.
	  ○ Driver's license numbers
	  ○ Passport numbers
	  ○ National identification numbers
	• Individual financial account numbers, such as:
	  ○ Bank account numbers
	  ○ Credit card numbers
	  ○ Or other information if that information would permit access to an individual's financial account.
	• Individual medical records, genetic information and biometric information, including information which is categorized as "Protected Heath Information" under the United States Health Information Portability and Accountability Act.
	  ○ Protected Health Information is defined by HIPAA as *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
	  ○ Individually identifiable health information is information, including demographic data, that relates to:
	  ▪ The individual's past, present or future physical or mental health or condition
	  ▪ The provision of health care to the individual
	  ▪ The past, present, or future payment for the provision of health care to the individual

	▪ The individual or for which there is a reasonable basis to believe it can be used to identify the individual. ▪ Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). • Consumer reporting data, including employment background screening reports and other information subject to the Fair Credit Reporting Act in the United States and similar legislation in other countries. • Data, regarding European Union residents, is classified as "Sensitive Categories of Data" under European laws and consisting of: ○ Race or ethnic origin ○ Political opinions ○ Religion ○ Trade union membership ○ Sex life or sexual orientation ○ Physical or mental health ○ Criminal charges or records related to criminal offenses and allegations of crimes. **Note –** While the combination of a client employee's name, address and email uniquely identify an individual, thus is considered Personal Information and ADP Confidential, this information MAY be used in unsecured emails to conduct normal business.
ADP Restricted	information is characterized as highly sensitive information which is intended for a very limited group of individuals who should be specified by name. This level contains information, which if disclosed would provide access to business secrets and could jeopardize important interests or actions of ADP or its clients and would be to the serious personal or financial detriment if revealed to unauthorized persons. Information should be classified as Restricted if it includes at least one of the following characteristics: • Strategic planning information, prior to general or public disclosure • Information on mergers, acquisitions or divestitures, prior to general or public disclosure • Financial forecast or results, prior to general or public disclosure • Information pertaining to business strategy • Any other information that may be damaging to ADP, if disclosed • Source Code (example: next generation application that will significantly advance client sales and retention.)