

# Accenture Employee and Contractor

# Client Data Protection Rules of Behavior

These Client Data Protection Rules of Behavior re-affirm our collective commitment to existing Accenture policies—they do not create new policies. Please read the following carefully, and consult the Accenture policies cited below if you need additional information.

If you believe that you do not or cannot comply with the rules identified below, you need to become compliant. Contact your supervisor for help and to obtain guidance on how you can bring your data protection practices in line with Accenture policy.

I understand and will follow these rules for protecting Client Data, including:

* **Personal Data**— any information that identifies or can be used to identify, contact or locate an individual, and any other information about that individual that is linked to such identifying information;
* **Business Data**—non-personal business information that is considered confidential by the client (e.g., financial information, trade secrets, etc.); and
* **Intellectual Property (IP)**—e.g., copyrighted, trademarked, or other protected materials, processes, designs, or trade secrets owned or licensed by the client.

1. **I will read and comply with the following specific Accenture Policies, and will consult my supervisor if I need help interpreting any of their requirements:**

* **11—Use of Accenture Delivery Methods**
* **51—Use and Distribution of Packaged Knowledge**
* **53—Non-Company Access to Company Systems**
* **56—System Security**
* **57—Security of Information and Acceptable Use of Systems**
* **69—Confidentiality**
* **91—Intellectual Property**
* **123—Archives and Records Management**
* **1253—Internal Distribution of Company Confidential and Material Non-Public Information**

II. **I will use care to identify and remain aware of any Client Data that resides on my individual devices, including:**

* Accenture –owned and/or personal electronic equipment (e.g., computers, external hard drives, personal files on shared servers, etc.),
* Portable data storage devices (e.g., PDAs, CDs, DVDs, flash drives, cell phones, etc.),
* Old and archival data and backups, and
* Information stored in hardcopy, (e.g., paper files, day planners, etc.).

I will provide my supervisor accurate information about Client Data under my control as requested.

1. **I will not use or retain any Client Data from a prior project**. Following the end of each project I will remove all Client Data associated with that project from the hardware and media under my control. If, during my current project, I find Client Data that appears to be from a different client, I will notify my supervisor immediately.
2. **I will access, use, disclose, and retain Client Data only as necessary to provide services for the client who owns the data.** I will not access Client Data that I do not need in order to perform my duties. I will use good judgment when collecting, using or disclosing Client Data in order to keep it secure and confidential. I will observe the “rule of least privilege” by not allowing others to access Client Data under my control unless they have a legitimate need for it and are assigned to my project. I will never use or disclose Client Data for personal purposes, or transfer such information to systems controlled by other clients.
3. **I will take all reasonable steps to protect Client Data in my custody.** I will follow all client and Accenture requirements related to information security, and will be responsible for implementing those requirements with respect to the Client Data under my control (e.g., use and protection of passwords, use of encryption, etc.). I will escalate threats to Client Data, or concerns about the adequacy of controls, to my supervisor.
4. **I will delete or destroy all Client Data when required or when it is no longer needed for business purposes.** I will not retain unnecessary copies of Client Data for any longer than needed to perform services for the client who owns the data, and will delete it when it is no longer needed. I will securely delete and overwrite Client Data from electronic media and will shred or otherwise permanently destroy hardcopies.
5. **I will observe all rules and restrictions when adding documents to the Knowledge Exchange (KX) or Accenture Records Management System (ARMS).** I will observe Accenture Policy 0123—Archives and Records Management. When I leave a project, I will provide copies of project materials to the project records management lead, and delete or destroy all Client Data associated with that project still in my possession, other than client contact information.
6. **I will follow the established incident response procedures for identifying and escalating security breaches affecting Client Data**. I will report known or suspected data breaches to the Accenture Security Operations Center (ASOC) at (+01) 202.728.0645, and also as directed within the project. A security breach includes any loss of control of Client Data, whether intentional or accidental, and can include lost or stolen portable data storage devices, misdirected data, computer hacking, or intentional misuse of Client Data. I will report suspected intentional misuse of Client Data immediately.
7. **I will consider the privacy of individuals when designing systems that utilize Personal Data.** I will seek to create privacy-protective systems and services consistent with client objectives. I will consider the privacy impact of my work and will take a conservative approach to the collection, use and disclosure of PII when developing solutions.
8. **I am responsible for my compliance with these Rules of Behavior and Accenture policies and procedures.** I understand that complying with Accenture policy also means complying with laws and client instructions. I understand that preserving the confidentiality and privacy of Client Data is a critical part of my job duties. I will conform to all Accenture policies and procedures with respect to the management of company or client data.

**Additional responsibilities of Accenture Supervisors:**

XI. I am responsible to make a reasonable effort to be aware of all Client Data in all systems, workstations, and electronic media under my authority, including individual user resources (e.g., laptops and portable media), and archival data and backups.

XII. I am responsible for regular, periodic review of my project’s Client Data inventory. At a minimum, Client Data will be inventoried when the following major events occur: (a) new systems or applications coming online, (b) new legal requirements taking effect, (c) after upgrades, restores or rebuilds resulting from a security incident, or (d) every year, whichever occurs first.

XIII. I will give proper attention to any issues related to information security or the misuse of Client Data that are escalated to me

XIV. I will implement and document procedures that govern the receipt and removal of hardware and electronic media containing Client Data, including equipment reassignment, and final disposition of equipment.

XV. I will be responsible for ensuring and confirming that required procedures are followed with respect to all security breaches affecting Client Data under my management.

Name: SOMNATH MUKHERJEE

Company: ACCENTURE

Title:

Date: OCTOBER 19, 2016

I acknowledge that I have read this document, understand its requirements and confirm that I will make my best efforts to comply with these rules: ⌧