

## Protecting Client Confidential Information

Deloitte is committed to protecting our client's confidential information, including personally identifiable information and sensitive business information. Deloitte's Office of Confidentiality and Privacy fosters a culture that emphasizes the importance of protecting our clients' confidential information. This Office sets guidelines, develops procedures, provides consultation and training, and assesses the effectiveness of controls, in each case, relating to confidentiality and privacy. The Office of Confidentiality and Privacy works in concert with Deloitte's Information Technology Services (ITS), including Cyber Security, and the Office of General Counsel to understand, prepare for, and respond to known and reasonably anticipated risks and threats facing our environment.

Consistent with industry leading practices for protecting confidential information, Deloitte has taken steps to remain *secure, vigilant, and resilient*, including:

- Understanding the risk environment
- Implementing policies, procedures, and controls designed to protect confidential information
- Responding to potential confidential information incidents in a timely manner
- Preparing and implementing plans to promptly recover from, and restore any of our systems that may be adversely impacted by, a cyber incident
- Actively monitoring the effectiveness of specific controls



**Technology Controls.** We use industry leading technology safeguards to protect confidential information, such as multi-factor authentication, whole-disk encryption on Deloitte-issued laptops, USB encryption technology, strong passwords, and data loss prevention technology on Deloitte-issued devices. Our professionals benefit from 24/7 security and technology support, which is accessible from around the world. Insider threat monitoring (detailed below) adds an additional layer of technology controls.

**Training.** The education process starts early as Partners, Principals, Managing Directors and other professionals are on-boarded at Deloitte. Thereafter, at least annually, Deloitte provides mandatory training that includes, among other topics, how to recognize various types of

confidential information, including personally identifiable information, and how to protect confidential information throughout the data life cycle (i.e., access, collection, transfer, storage, deletion, and retention). Our professionals are also trained to recognize various types of cyber risks and threats; report suspected and actual incidents that could impact our clients or the Deloitte organization (e.g., affecting brand, reputation, or physical safety of persons); and locate Deloitte reference materials (e.g., policies, web sites, and contact information).

**Policy.** Deloitte's policies are accessible to our professionals on our intranet. Among other things, our policies address ethics and compliance, physical security and safety, privacy and confidentiality, and copyright and intellectual property. Our professionals acknowledge compliance with key policies twice per year.

**Awareness.** Subject matter leaders from the Office of Confidentiality and Privacy and Information Technology collaborate as a team and issue frequent internal communications throughout the organization. These communications—guidance, specific reminders, notices, and tips—pertain to, among other topics, new threats affecting the cyber risk landscape and to specific controls relating to confidentiality, privacy, and security.

**Data Transfers.** The security and privacy of data transfers is critical to our business. We evaluate cross border and domestic transfers of confidential information, including personally identifiable information, and apply appropriate safeguards and legal mechanisms when required. Additionally, Deloitte adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to personally identifiable information that is transferred from the European Economic Area, the United Kingdom and Switzerland to the United States.

## Vigilant.

We conduct active and ongoing monitoring of external threats as well as internal or “insider” threats, leveraging security and behavioral cognitive technologies.

**Externally.** To protect us from external threats, our vulnerability management services help decrease the exploitable gaps in software and hardware configurations, while our application risk monitoring helps to enable visibility into the risk posture of critical applications and business processes. Our intelligence and analytics provide awareness of our current

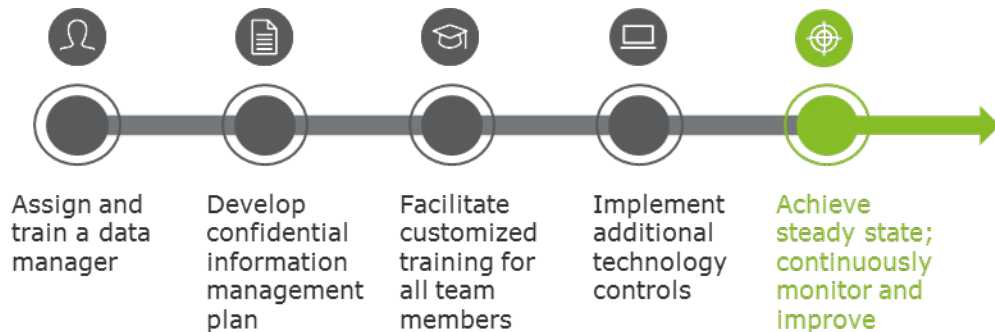
landscape and insight to further improve threat detection.

**Internally.** Deloitte’s Insider Threat Program (ITP) is a holistic, proactive, risk-based program that incorporates technical tools, controls, business processes, policies, and trainings necessary for deterring, detecting, and mitigating insider threats. Deloitte defines an insider threat as professionals, contractors, or other third parties accessing and/or using our systems, who, given their access to people, information, assets, or facilities, could adversely affect Deloitte’s business continuity, financial standing, reputation, or employee safety due to ignorance, complacency or malicious acts. Deloitte’s primary ITP focus areas include espionage, sabotage, confidential information and intellectual property theft, fraud, workplace violence, security compromise, and physical property theft.

## Resilient.

Being resilient means having the ability to recover from, and mitigate the impact of, incidents. Because it is not possible for any organization to entirely eliminate the possibility of an incident, we practice internal planning and readiness, much like we assist clients in planning for, responding to, and recovering from, cyber incidents that have the potential to seriously disrupt operations, damage reputation, or destroy enterprise value. We continue to evaluate and work to improve our incident response preparedness and technical capabilities to recover from disruptions to technology.

**The Confidential Information Program.** Deloitte has designed and implemented a Confidential Information Program which provides a consistent, flexible, and scalable method for effectively mitigating confidentiality risks within our client engagement environments. The program is deployed at client accounts, engagements, and supporting business areas based on the risk and nature of our services (e.g., consulting on a merger or acquisition) or where we encounter, among other things, sensitive information, large volumes of confidential information, or unusually strict data handling requirements in the delivery of our services. This helps us to maintain our clients' trust and proactively safeguard our clients' reputation as well as ours. The typical process we use to implement the program is outlined below.



A team member (Data Manager) from the account or engagement team is identified by the account or engagement team leaders. The Data Manager creates an account or engagement confidential information management plan which includes administrative, physical, and technical safeguards to be implemented by the account or engagement team to protect client confidential information throughout various stages of the data life cycle.

After the plan is agreed to by Deloitte account or engagement team leadership, the Data Manager oversees the implementation of the confidential information management plan on the account or engagement, which includes training team members. Ongoing processes, such as training new team members, performing engagement or account on-boarding and off-boarding duties, and monitoring compliance, are performed by the data manager and his/her delegates.

### About Deloitte

As used in this document, "Deloitte" means Deloitte USA LLP, Deloitte LLP and/or their respective subsidiaries. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.