Ogletree Deakins

The sample forms provided as part of this presentation are intended merely for informational purposes. No representation is made as to the enforceability of these forms in any jurisdiction, and the materials should not be relied upon or construed as legal advice, or as a substitute for obtaining legal advice from an attorney licensed in the applicable jurisdiction(s).

Protection of Confidential and Trade Secret Information Best Practices Checklist[1]

ON BOARDING PROCEDURES

In General:

- Review language in all agreements/policies to ensure that they are narrowly tailored and specific as to the categories of confidential and trade secret information ("information") covered.
    - Confidential information may include but is not limited to information provided by or shared between customers, employees and third parties such as service providers, vendors and contractors.
- Review language in all agreements/policies to ensure that employees are aware of consequences for failing to protect information, including disciplinary action.
- Ensure that confidentiality agreements/policies clearly state that information is not to be deleted from company-issued devices and such devices are not to be formatted before they are returned at the end of employment.
- Include language in policies and agreements notifying employees that [COMPANY] has the right to conduct surveillance of employee conduct while using [COMPANY] property (e.g. monitoring [COMPANY] laptops and mobile phone) and while on [COMPANY] property (e.g. surveillance cameras in work spaces or parking lots) to the extent permitted by law.
- Include language in documents during the hiring process (e.g. conditional offer letters) that background checks and references will be checked to the extent permitted by law.
- Include Defend Trade Secrets Act (DTSA) Notice of Immunity in relevant agreements/policies

[1] This checklist summarizes best practices based on US legal requirements only.

- Conduct legally compliant background and reference checks on employees and require that third party vendors and other service providers conduct checks for their workers who have access to [COMPANY] information based on financial industry standards. For example, for workers covered by Section 19 of the FDIC, consider criminal background screening which includes the period between the individual reaching the age of 17 and the present.

Third Party Vendors and/or Service Providers:

- Require confidentiality agreements or include confidentiality provisions in service provider and other similar agreements before sharing or allowing access to information with vendors, consultants or contractors, including with temporary staffing agencies, SOW or other temporary workers which requires the same level of safeguards for the protection of confidential/trade secret information as those required by [COMPANY] for its own operations.

- Review the written information security plan for service providers which documents that they have implemented comparable security measures to safeguard [COMPANY]'s confidential/trade secret information.

- Conduct periodic audits of service providers who have received confidential/trade secret information to ensure compliance with [COMPANY] security standards and protocols and receive assurance that timely corrections will be made to areas of risk.

Employee Agreements

- Signed Confidentiality/Non-Disclosure Agreement

- Signed Restrictive Covenants Agreement (as applicable)
  - Noncompete
  - Non-solicit of employees
  - Non-solicit of customers

- Signed Assignment of IP Agreement (as applicable)

Workplace Policies

- Confidentiality/Non-Disclosure

- Privacy

- Social Media

- E-mail
- Internet
- Passwords
- Smart Devices
- Return of [COMPANY] Property
- Telecommuting
- IT Security
- Acknowledge Receipt of Employee Handbook
- Acknowledge Receipt of Code of Conduct

Training and Education

- Review confidentiality agreements and policies during new-hire orientation and on-boarding process. This training should be provided to third party contractors, statement of work, temporary staff and consultants as well.
    - Discuss what types of information are considered confidential and trade secrets and how such information should be transmitted, if at all.
    - Emphasize importance of protecting information and the consequences of not doing so including potential discipline, civil action and/or criminal prosecution.

DURING EMPLOYMENT

Risk Analysis

- Establish the chain of custody of all categories of information.
    - Identify all of the employees, departments, functions and/or third parties that come in contact with the data from the moment the information is obtained or developed,
- Conduct a risk analysis of each department which has access to different categories of information and assess the effectiveness of safeguards to protect the information in each department.

- Categorize information by type and confidentiality level. For example, assets may include intellectual property; internal protocols and procedures; financial projections or summaries; research data; specific databases; and customer and/or employee lists. Among these categories, some documents may be classified as "important" (i.e., email lists and non-financial business information), "confidential" (i.e. customer information, pricing, contract terms, margins, business plans), "private" or "personal identifiable information (PII)" (i.e. employee records) or "crucial" (i.e. trade secrets, formulas, sensitive financial and customer information).

- Identify categories of information which may require specific safeguards required under state, federal or foreign law (e.g. social security numbers) and assess whether current protections are adequate.

- Establish or baseline an existing IT security program using nationally and internationally recognized cybersecurity and risk management frameworks, including but not limited to those created by the National Institute of Technology (NIST) https://www.nist.gov/ and/or ISO 27001, CoBIT, PCI DSS, FISAP SAP.

Written Information Security Program (WISP)

- Document all processes and procedures taken to safeguard confidential and trade secret information from on-boarding (see above) through post-employment (see below).

- Develop a tiered system for access to information which is role-based, so only certain employees have access to only certain information necessary to do their work (e.g. "first level security," "second level security," and "third level security" for allowing access to confidential and trade secret information).

- Develop specific procedures for categories of information which require special protection based on legal requirements (e.g. social security numbers and PII of EU citizens).

- Create and comply with a data retention policy which tracks and documents when files are destroyed.

- Develop written procedures for reporting suspicious competitive activity during employment and post-employment.

    - Procedures should include maintaining a log of suspicious patterns and activities (e.g. communications between an employee and direct competitors.)

- To the extent software is developed, ensure that an enterprise software development program is established using a documented software development lifecycle (SDLC) process that embeds security throughout.

- Create a written Incident Response Plan which can be included in the Disaster Recovery Plan or Business Recovery Plan.

    - The Incident Response Plan should include appropriate incident notification, containment, investigation, and recovery procedures.

    - Create an Computer Incident Response Team (CIRT) to immediately respond to and address any potential data security incidents or issues.

- Formally designate at least one employee to manage the WISP and ensure compliance.

- Identify points of contact in Human Resources, IT, Security and Legal to understand the scope of the WISP and enforce agreements and policies consistently throughout the organization.

- Join financial services industry consortiums and organizations focused on reducing cyber-risk, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), https://www.fsisac.com/.

Periodic Audit

- Routinely monitor and test the WISP to ensure the information is secure, including creating an audit trail that documents who, when, and for what purpose data (including hard copies) was accessed.

    - If issues are identified, document how issues have been corrected.

- Change the safeguards as needed with the changes in how information is collected, stored, and used.

- Conduct IT system assessment including diagnostics runs and external audits regularly to ensure integrity of system, particularly when significant changes are made to the network infrastructure.

- Review and update all confidentiality and security agreements with employees and ensure signed copies on file every _____.

Training and Education

- Basic training and acknowledgement of [COMPANY]'s confidentiality policies occurs every __years.

- Remedial training available for those who have violated policies/agreements.

- Routinely raise awareness as to why confidentiality is important, how confidential information is classified, how to handle confidential information and, finally, how to resolve any questions or issues that may arise involving confidential and trade secret information, particularly in light of new external threats (e.g. phishing scams).

- Provide "cheat sheets" on how to identify, label and store confidential information to employees.

- Promptly pass along information and instructions to employees regarding any new security risks/

Data Security

Data Protection and Encryption

- Include a watermark on all confidential and trade secret documents as such, e.g. "Confidential" or "Trade Secret."

- Restrict the use of external hard drives or USB devices to store [COMPANY] information but if needed, encrypt confidential and trade secret data stored on such devices.

- Disable unneeded USB and DVD ports.

- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.

- Turn off computers at the end of the work day.

- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing confidential information.

- Encrypt categories of information when stored on [COMPANY] devices. Categories include but are not limited to:

    - [COMPANY] Intellectual Property or Proprietary Data
    - [COMPANY] Financial Reports
    - Personally Identifiable Information

- Research and Development Data
- Sensitive Customer Data
- Upcoming Product Launch Details

- Encrypt the transmission of confidential information over unsecured connections, such as the Internet.

- Encryption keys must be stored outside the cloud environment and managed by someone besides the cloud services provider.

Network Security

- Install operating system updates and patches that resolve software vulnerabilities.

- Use anti-virus, anti-malware and anti-spyware software that updates automatically on [COMPANY] devices and require employees to install such software on personal devices which access [COMPANY] information.

- Use data leak protection software.

- Implement gateway filtering of email.

- Install web filtering software.

- Use an up-to-date intrusion detection system which provides alerts of attacks.

- In co-mingled processing environments and databases, implement logical or physical segregation of data and methods to assure data is not viewable by unauthorized end-users.

- Avoid using public Wi-Fi to access [COMPANY]'s confidential information.

- Prohibit use public cloud services such as Dropbox, Google Drive, or iCloud for sharing or backing up work on [COMPANY] matters and personal accounts should not be used to access those cloud services.

- Review all physical locations, by country, where technology will be utilized to provide cloud storage and retrieval services. Confidential and trade secret information should remain in the original country of origin and the location of all such information must be known at all times.

Password Management

- Require that all [COMPANY] information, including passwords, be stored on secure and backed-up [COMPANY] networks and not on desktops, personal devices or unsecured drives.

- Require password-activated screen locking after period of inactivity for all [COMPANY] devices and personal devices where [COMPANY] information transmitted or stored.

- Use "passphrases" or strong passwords for internet and server access, and require that they be periodically changed.
    - Passphrases: a series of random words or a sentence. The more characters the passphrase has, the stronger it is.
    - Consider strong passwords which require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.

- Use Two Factor Authentication and Multi-Factor Authentication for [COMPANY] devices or personal devices which can access [COMPANY] information.

- Users who are outside [COMPANY]'s network or VPN should be sent a numeric passcode by email as part of log in procedure to access [COMPANY] networks.

- Practice the Principle of Least Privilege (PoLP).
    - Do not log into a computer with administrator rights unless necessary to perform specific tasks.

External Transmission

- Prohibit transmission of business information to and from personal e-mail addresses.

- Block export of unencrypted and unauthorized data through out-bound e-mail.

- Use a Secure Sockets Layer (SSL) or other secure connection, so that the confidential information is protected in transit.

- Caution third parties, service providers, customers or clients against transmitting confidential data via email or in response to an unsolicited email or pop-up message.

Remote Access

- Restrict use of personal electronic devices (including personal phone and laptops) to conduct business unless there are safeguards meeting appropriate security standards.

- Ensure that [COMPANY] laptops, PDAs, cell phones, or other mobile devices (including personal devices accessing [COMPANY] information) are stored in a secure place when not in use.

- Enable remote wiping of [COMPANY] information stored on company-issued electronic devices or employee's personal devices which access [COMPANY] information.

- Require that telecommuting and home offices include the same or comparable level of security as in-office work environments.

- Where possible, avoid storing sensitive customer data on a computer with an internet connection.

Monitoring and Surveillance

- Conduct surveillance and/or monitoring of [COMPANY] computers and devices for suspicious activity including:
    - forwarding of [COMPANY] documents to personal email accounts
    - attempting to bypass a particular security system on more than one occasion
    - communications between an employee and direct competitors.

Physical Security

Physical Access Controls

- Physically secure confidential documents and trade secrets in locked and/or restricted areas (e.g. locked drawers).

- Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.

- Situate fax machines in secure or limited access areas; use pre-coded phone numbers to eliminate dialing errors; use cover sheets so information is not physically exposed; testing fax machines periodically to ensure numbers are correct and functions are working properly; de-programming fax memory storage after use to prevent recovery of confidential information.

- Remind employee that they cannot leave confidential information on desks, printers, unsecured work spaces, garbage cans, or flash drives where others could view, download, or copy such information.

Internal Facility Security

- Install surveillance cameras and/or close circuit television (CCTV) in areas where confidential and trade secret information is stored or used (such as open workspaces and kiosks) as well as entrance/exit doors.

- Install on-site and off-site alarm monitoring and security officer/guard services.

Visitor Management

- Implement employee and guest access control procedures to restrict access to areas where confidential and trade secret information are routinely maintained, such as through access control badges and photo identification badges.
- Maintain procedures and processes for managing, tracking, and logging visitors (i.e., visitor management) to and within all facility(s) and environment(s).

Document Management

- Stamp and mark confidential documents as such, e.g. "Confidential" or "Trade Secret."

- Create a form tracking log for any external disclosure of confidential and trade secret information or a sign-out system for internal use of such information.

- Implement policies/procedures for safe transfer of physical documents from one physical location to another, including outside of secure department or location.

- Establish shredding policies/procedures for disposal of documents after use which ensures the information cannot be read or reconstructed.

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information.
    - conduct due diligence beforehand of any outside disposal companies by checking references or requiring that the [COMPANY] be certified by a recognized industry group.

- Maintain an inventory of [COMPANY] computers and any other equipment on which customer information may be stored.

EXIT PROCEDURES

In General

- Internal Communication:
  - Send announcement to entire office within a week of last day if possible.

- External Communication:
  - Notify clients/vendors if employee had direct contact and inform them of new contact.

- Review Departing Producer Checklist (attached).

- IT Tasks on Last Day of Employment (complete on or before exit interview):
  - Shut off on-site and remote access to computer, server, voicemail and email.
  - Obtain and hold computer or laptop. Do not turn it on in the event there is a need to forensically obtain evidence.
  - Identify all critical files and save on server and/or USB flash drive.
  - Notify IT to route voicemail and email to a designated person for a short period of time before voicemail and email is turned off.

Exit Process and Interview

- Workflow:
  - Review work that needs to be transitioned and determine point of contact.
  - Ask employee to document processes, project status, etc.

- IT Information from Employee:
  - Obtain from employee passwords to VM, email, computers, phone or other [COMPANY] devices.

- Use Return of [COMPANY] Property Checklist (attached).

AFTER EXIT INTERVIEW

- Do not allow employee to return to his office unaccompanied.
- Do not allow employee to return to sit in front of his computer.
- Do not allow employee to take anything from his office – other than immediate necessary items, *i.e.*, car keys, wallet, bag (but check inside for [COMPANY] property).
- Do schedule date to deliver all personal effects to Employee.
- Do schedule date for pick-up of any [COMPANY] property in Employee's possession.

- Do escort employee from the building.

CONTACT LEGAL IF:

- Employee has one of the following titles: _____
- Employee has access to significant confidential information.
- Employee is leaving for a competitor.
- Employee refuses to say where he/she is going to work next.

If you have any questions about this form, please contact: Katy Yang-Page | Miami, FL | Telephone: 305-455-3704 | E-mail: katy.yang-page@ogletree.com or Todd Kaiser | Indianapolis, IN | Telephone: 317-916-2155 | E-mail: todd.kaiser@ogletree.com

© Ogletree, Deakins, Nash, Smoak & Stewart, P.C.