Employment Termination Policy

www.veriato.com

Veriato

Employment Termination Policy

When an employee's relationship with a company is terminated, whether voluntarily or involuntarily, it is the responsibility of the company to ensure not only a smooth transition for the departing employee, but to safeguard the company's assets. Carnegie Mellon University's Computer Emergency Response Team Program, CERT, states concerning "an employee's departure, organizations must address a number of areas before the employee's last day. Organizations must develop policies and procedures that encompass all aspects of the termination process."[1]

SpectorSoft offers guidance in creating a strong Employment Termination policy, covering the employee and the treatment of corporate assets related to the employee, to help mitigate the risk of theft or loss.

When creating a Termination of Employment policy, SpectorSoft recommends you keep the following in mind:
1. A solid Termination of Employment policy starts with the Onboarding process
2. Each position within the company should have an assigned insider threat risk level, with applicants of higher risk positions requiring more thorough pre-hire investigation as well as sufficient activity monitoring once onboard
3. Certain job categories require more active review than others

Be sure legal counsel familiar with your company as well as local and federal regulations reviews any policy before enacting it. The suggestions provided within this document, such as the sample policy in Appendix C, are a guideline and should be used as a springboard to create effective policies that are appropriate for your business.

Employee Onboarding

While there is no one-size-fits-all policy to cover every situation, setting a positive tone for the employee/employer relationship from the outset is critical. According to the CERT Common Sense Guide to Mitigating Insider Threats, "An organization's approach to reducing its insider threat should start in the hiring process."[2]

[1] Carnegie Mellon University Software Engineering Institute. Common Sense Guide to Mitigating Insider Threats 4th Edition (CMU/SEI-2012-TR-012 | 65) December 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

[2] Carnegie Mellon University Software Engineering Institute. Common Sense Guide to Mitigating Insider Threats 4th Edition (CMU/SEI-2012-TR-012 | 23) December 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

SpectorSoft believes the following actions are crucial to keeping corporate Intellectual Property (IP) safe throughout the employment lifecycle:

1. Create and maintain a list of corporate services for each employee
2. Review expectations related to corporate IP, including the Confidentiality and Intellectual Property Agreement (CIPA) each employee must sign
3. Provide an Employee Handbook outlining the Acceptable Use Policy related to corporate IT resources

List of Employee Services

Regardless of your company's size, every employee will be given access to certain corporate assets and services. Taking the time to define each position within the company, creating both a job description and a standard template of corporate services for the position, pays great dividends later in the employee lifecycle. Corporate services can include, but are not limited to:

- Access to corporate networks and drives
- Passwords for all company applications
- Company social media account credentials
- Keys to offices, parking passes, etc.
- Corporate credit cards or purchasing cards
- Physical assets such as phones, laptops, or tablets

As the breadth of an employee's responsibility grows, so may the services the employee can access. SpectorSoft urges you to track these services carefully. During onboarding, create a living document of employee services using the predefined template for the position as a starting point. This document should be owned by the employee's manager and reviewed regularly, ensuring all corporate services available to the employee are documented.
A more detailed List of Services sample is provided for you in Appendix A.

Expectations Related to Corporate IP

Reviewing the treatment of corporate intellectual property is a critical onboarding process some companies overlook. Surveys show that 40% of employees have taken an employer's corporate information to a new company when changing jobs[3]. During onboarding, set the expectation that information such as source code, customer lists, product details, and financial statements are the exclusive property of the company. Keep in mind many employees have a sense of entitlement to company IP they helped to create. For example, as a salesperson builds a list of contacts, the feeling that the employee owns their work product is common. The CERT Guide to Insider Threats discusses this phenomenon in reference to the Entitled Independent, an insider acting primarily alone to steal information to take to a new job or to his own side business.

[3] Symantec. "What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk", February 2013

"The employee comes into your organization with a desire to contribute to its efforts. As time goes on and he develops information, writes source code, or creates products, his contribution becomes more tangible. These insiders, unlike most employees and contractors, have personal predispositions that result in a perceived sense of ownership and entitlement to the information created by the entire group. The longer he works on the product, the more his sense of entitlement grows."[4]

Regardless of the Entitled Independent's perception, the company provided the time and resources, financial or otherwise, with which the list was cultivated, making that list the company's asset. During onboarding, set the expectation that employees will be required to return and destroy copies of corporate assets and intellectual property they have in their possession. Employees should sign a Confidentiality and Intellectual Property Agreement (CIPA) upon hiring, which will outline the acceptable use and disposition of corporate IP. Although the CIPA should be broad enough to protect the company from a range of situations, ensure it covers the concept that source code, client lists, product lists, design specifications, etc. are the exclusive property of the company. Additionally, consider a statement that clients and vendors are proprietary to the company, and any future solicitation would be considered a breach of the agreement. This may be accomplished via a non-solicitation agreement. Legal counsel can assist in determining the best approach for your organization.

It is no longer enough to ask departing employees to return copies of information. In the digital age, employees can easily move IP from your network to USB drives (thumb drives or flash drives), the cloud (DropBox, iCloud, etc.) or their own devices. Be very clear that employees are expected to return and destroy any copies of the company's intellectual property they may have. Additionally, as mentioned above, setting expectations during the onboarding process with keep employees mindful that IP is the property of the company, and must be treated as such.

In Appendix B, you will find a sample of items SpectorSoft suggests as critical corporate Intellectual Property to protect.

[4] Dawn M. Cappelli, Andrew P. Moore, Randall F. Trzeciak. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). January 2012

Review of Employee Handbook

Whether a large company with a formal document, or small businesses with a one page list of "Dos and Don'ts", providing employees with guidelines for acceptable behavior is essential. The CERT Common Sense Guide to Mitigating Insider Threats clearly states "Organizations must communicate their policies and practices to new employees on their first day. Such policies and practices include acceptable workplace behavior, dress code, acceptable usage policies, working hours, career development, conflict resolution, and other workplace issues."[5]

The vast majority of employees want to work hard, contribute to company success, and "follow the rules." Clearly spelling out company rules makes it easier (and less stressful) for them to do so. Consistently enforcing your company rules is also critical. Keep the "Broken Window" theory in mind. When little things, like a broken window, are quickly addressed larger problems, like vandalism escalating into more serious crime, tend not to materialize.

During the onboarding process provide the employee handbook to new hires, and have them acknowledge receipt of this document. When acknowledging receipt of the employee handbook, call attention to the fact that corporate IP (in essence all employee work product) must be returned and/or destroyed should the employee leave the company.

Assess the Insider Threat Risk of Each Employee

Inherent to each position within your company is a certain amount of risk related to insider threat. The risk will vary not only from position to position, but also from employee to employee within the same position. SpectorSoft recommends establishing an insider threat risk baseline for each position within the company. Once this baseline is established, management can then determine what measures, if any, should be taken to monitor the employee's computer activity in order to protect the company's intellectual property.

The assessment of insider threat risk does not stop after the onboarding process. Management should continually assess employee risk. Evaluate the employee's sentiment about the company, any personnel issues affecting the employee directly or indirectly, signs of stress (especially financial) in their personal lives, and changes to their work patterns. Anomalies in any of these areas could be an early indication of insider threat. The next section will cover several key positions that carry a high inherent risk of insider threat.

[5] Carnegie Mellon University Software Engineering Institute. Common Sense Guide to Mitigating Insider Threats 4th Edition (CMU/SEI-2012-TR-012 | 28) December 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

While smaller companies may not have many distinct departments, SpectorSoft realizes it is the information these departments would handle that is targeted for theft. Therefore, careful attention should be paid to employee terminations occurring within the following departments:

- **Finance Department** – access to bank information, confidential financial documents
- **HR Department** – access to sensitive employee and payroll data
- **Sales Department** – access to customer lists, product information
- **IT Department** – access to all systems where confidential information is stored

The CERT Common Sense Guide to Mitigating Insider Threats states "organizations should conduct a review of the departing employee's online actions during the 30 days prior to termination [Hanley 2011b], and the 30 days before and after the date of a notice of resignation, if that date is different from the termination date. This review should include email activity to ensure that the employee has not emailed sensitive company data outside the organization, such as to a personal email account or a competitor." Having an effective employee monitoring solution in place eliminates the rush to review old email and activity, or to begin monitoring once the employee termination process begins.

Certain Job Categories Require More Active Review Than Others

Consideration should be given to the amount of insider threat risk a departing employee carries. This risk varies based on the employee's job category, and will impact the method of employee activity monitoring deployed. For example, a resigning staff accountant who handles a limited number of journal entry transactions likely requires less scrutiny than an assistant controller who has access to the entire chart of accounts, financial statements, and banking information. Therefore, consider the following categories when setting up an employee monitoring solution to mitigate IP theft and insider risk:

- **Corporate Officers** – often privileged to have the most confidential information
- **Controllers, Assistant Controllers and Treasurers** - have broad access to the company's financial information
- **Developers / Programmers** – review code for malicious intent or "back door access", as well as making sure no source code has been copied or otherwise exfiltrated
- **Database Administrators (DBAs)** – ensure that access is secure from within and outside of the corporate network. Ensure confidential information within the database is safeguarded and access to it is monitored
- **System Administrators (SysAdmins)** – monitor privileged accounts as well as ensure no new accounts have been created recently that may serve as a way in to the company post-termination

• Contractors – a strong Bring Your Own Device (BYOD) policy will aid in securing IP when working with contractors. Ensure contractors sign, acknowledge and abide by confidentiality agreements, and are aware of the expectations set out in the employee handbook section above

Due to some positions having higher risk than others, SpectorSoft recommends a blended approach to employee monitoring.

A passive employee activity monitoring solution, such as Spector 360 Recon, records employee activity and generates alerts from events detected in the employee activity logs. However, the data collected is not available for review, reporting, or retention unless there is cause and subsequent authorization to do so. This protects the privacy of the employee while protecting corporate Intellectual Property.

An active employee activity monitoring solution, such as Spector 360, records employee digital activity, making the collected data available for review, reporting, and retention to authorized reviewers. Active monitoring, sometimes referred to as employee surveillance, is typically employed where there is imminent threat to corporate assets and IP.

A blend of passive and active monitoring makes sense for many organizations—combining broad deployment of the passive capability with targeted use of the active monitoring capability as needed. Any of these monitoring strategies can accomplish the goals of protecting the corporate assets and interests during the termination of employment process.

Activity Monitoring Considerations During Notice Period

The broad deployment of passive activity monitoring provides the ability to review computer activity for the 30 days prior to the notice period. However, once notice has been tendered, consideration must be given to actively monitoring the employee.

If an employee tenders their resignation, and is not actively monitored, deploying an active employee monitoring tool will collect their computer activity, allowing the company to monitor and analyze activity during the notice period, and for a limited time after the employee leaves the company. Additionally, consideration should be given to monitoring those associated with the departing employee for a limited time, recording their computer activity for potential insider threats.

Once an employee is recognized as not performing at or above expectations, as well as employees carrying a higher risk of insider threat, deploying an active monitoring solution is recommended. A history of the employee's actions are securely recorded and analyzed, providing detail to support actions of termination if necessary. Additionally, evidence of any malfeasance will be quickly made visible, so appropriate action can be taken.

Whether an employee resigns, or employment is terminated for cause, an exit interview should be conducted as soon as practical after notice is given. When conducting an exit interview, be thoughtful of cues that could signal larger issues within the company. An employee offering that they were unhappy with management or company policies can indicate a potential insider threat. It may signal a need to monitor and review employee computer activity in order to protect corporate IP from threat, whether from the departing employee, their friends and even close associates within the company.

Every Employee Termination is Unique

It is not possible to predict how each employee lifecycle will play out. Some employees will retire after fruitful careers at the company. Others will choose to leave the company, giving notice that catches management by surprise. Finally, it is unfortunately the case that some employees will not work out, and termination of employment is necessary.

Regardless of what gives rise to these situations, employee activity monitoring is a vital component of safeguarding corporate intellectual property. SpectorSoft welcomes a partnership with your company to provide the employee monitoring solution that best fits your company's needs.

Appendix A
Corporate Services Matrix

Performing a periodic review of the services an employee can access will ensure proper safeguards of corporate intellectual property and data.

Employee Name	
Hire Date	
Services Review Date	

Service	User Name	Date Provisioned	Date Decommissioned
Corporate Network Access			
Accounting Program (Oracle, SAP, Quickbooks)			
Sales / CRM Program (SalesForce, ACT!)			
Corporate Social Media (Twitter, Facebook)			
Company Phone, Tablet			
Company Laptop/Desktop			
SQL Server Credentials			
Bank Account Access			
Human Resources Program (Workday, etc)			
Payroll Program (ADP, etc)			

Appendix B
Corporate Intellectual Property

SpectorSoft wants to aid in protecting your company's Intellectual Property (IP). IP is created through the expenditure of time and money, and should be safeguarded at all costs. Employee monitoring programs like Spector 360 can help protect your IP while your employees are still working for the company. However, once employment is terminated, it is critical to ensure the following intellectual property is secured:

- Client/Customer Lists
- Product Information
- Financial Information
- Programmer/Developer Source Code

It is no longer enough to ask departing employees to return copies of information. In the digital age, employees can easily move IP from your network to USB drives (thumb drives or flash drives), the cloud (DropBox, iCloud, etc) or their own devices. Be very clear that employees are expected to return and delete any copies of the company's intellectual property they may have. Additionally, as mentioned in above, setting expectations during the onboarding process with keep employees mindful that IP is the property of the company, and must be treated as such.

A sample Confidentiality Agreement can be found online. Resources such as IP Watchdog can provide a template. However, as with any policy or agreement, have legal counsel familiar with your business review the document before putting it in place.
http://www.ipwatchdog.com/tradesecret/standard-confidentiality-agreement/

Appendix C
Termination: Policy and Procedure

The below sample policy is meant as a guideline. It should be used as a starting place for your own company policy. As mentioned previously, be sure that policies enacted at your company abide by local and federal laws. A review by legal counsel is recommended.

Employment Termination Policy

1.0 Policy

It is Company policy that employee terminations are handled in a professional manner with minimal disruption to ongoing work functions. Termination of employment - whether voluntary or involuntary – marks the end of the employment relationship between the Company and the employee. Nothing contained within the Policy is intended to create legally enforceable contractual rights.

2.0 Voluntary Terminations

2.1 A voluntary termination occurs when an employee leaves a job on his or her own initiative. Voluntary termination of employment occurs when an employee informs his or her supervisor of employee's resignation, or termination is deemed to have occurred as a result of a predefined event. Examples of voluntary termination include but are not limited to:

- Resignation
- Retirement
- Contract Expiration
- Job Abandonment, such as

o Failure to report to work for X consecutive days without notice

o Not returning to work after leave status, such as FMLA

2.1.1 Upon receipt of written notice of voluntary termination of employment, resignation, the manager should immediately forward the notice to Human Resources.

2.2 When an employee resigns from the Company, it is expected that he or she provide sufficient notice. Though sufficient notice is a function of the position the employee holds, the minimum expectation is two weeks notice to allow for adequate training and transfer of responsibilities.

2.2.1 It may be deemed the best interest of the Company to accept the resignation of the employee and enforce it immediately. In lieu of the employee serving the period of notice, the Company may provide an amount of severance pay equal to the standard two-week notice period.

2.3 If it is deemed in the best interest of the Company to accept the resignation the employment immediately, the Company will ensure corporate asset checklists are met or prepared to enact protocols immediately are secure prior to notifying the employee of the immediate resignation.

3.0 Involuntary Terminations

An involuntary termination is one initiated by the Company, and includes a layoff or discharge.
Examples of involuntary termination include but are not limited to:

- Reduction of Force
- Termination for Cause

4.0 Employment At Will

It may be the case that the Company operates in a state that is considered an Employment At Will state. Employment At Will refers to the employee's right to terminate his or her employment relationship with the Company at any time and for any reason (or for no reason at all). Additionally, the Company has the right to terminate the employment of any employee at any time for any lawful reason, or for no reason at all. The employment relationship between the Company and its employees is at-will with the exception of those relationships covered by an employment contract. In those instances, the terms and conditions of the employment contract will prevail.

The Company will include conditions of "Employment At Will" in the Employee Handbook, should they be relevant.

5.0 Approval of Involuntary Termination

Human Resources must approve the involuntary termination of an employee. Terminating the employment of a Company officer must be approved by the Chief Executive Officer, President or Chief Operating of the Company. As corporate officers can do a disproportionate amount of damage to the Company in the event of theft or fraud, careful review of the officer's access to corporate services should be performed.

6.0 Coordination of Employee Termination

The HR Manager is responsible for the processing of all employee terminations. Processing includes

- Returning all company property noted in Checklist A
- Review of benefits status
- Completion of an exit interview questionnaire

7.0 Final Pay

The final pay for a terminated employee will be in the form of a check and will include the following: unpaid work time, overtime due, and the balance of unused Paid Time Off (PTO). Deductions from the final check will be made for benefit contributions, docked time, outstanding expenses, and fines for lost or missing Company property. The final paycheck will be issued within the following two (2) pay periods. In the event of a death, the final paycheck will be paid to the estate of the employee.

8.0 Corporate Services

It is the responsibility of the employee's direct manager to obtain any critical password and login information for Corporate Services. In the event the employee was a gatekeeper of information, such as a Database Administrator or Information Technology (IT) manager, the employee's manager should be sure to cover all services managed by the employee, including direct logins, remote logins, and "backdoor access" to all services. Checklist B contains a list of Corporate Services to consider for all employees.

Employees who possess a security clearance are required to check out and debrief with the Security Officer no later than their last day of employment.

9.0 Eligibility of Rehire

Certain employees who terminate voluntarily or who are laid off may be eligible for reinstatement at a later date.

Checklist A – Company Property

The following items must be returned to the Company by an employee once terminated

1. Employee ID card
2. Company issued phone(s)
3. Company issued computer(s)
4. Company issued tablet(s)
5. Keys to offices, doors, conference rooms, restrooms
6. Company issued parking permits

Checklist B – Company Services

The following services, as applicable, must be terminated by the Company once an employee is terminated

1. Access to corporate network
2. Access to corporate email
3. Access to corporate accounting/ERP system
4. Access to corporate budgeting/reporting packages
5. Access to all company databases
6. Social media, Cloud storage, etc.

Go to www.veriato.com for a Free Trial or email us at: sales@veriato.com

Corporate Offices

Veriato, Inc.
4440 PGA Boulevard, Suite 500,
Palm Beach Gardens, FL 33410
1.888.598.2788
1.772.770.5670

International

United Kingdom
C2, Dukes Street
Woking
Surrey, GU21 5BH
+44 1483 397744