Initech Acceptable Use Policy
Audit Plan

Sherlock Group
December 2015

Control Objective	Control Activities	Audit Procedures
CO-AUP-1 - Expectations for acceptable use are formally documented, reviewed and approved by Sr. Management, and made available to employees.	**CO-AUP-1-CA1** - The Initech Acceptable Use Policy document is reviewed and approved annually by the Initech Board of Directors. The policy is revised as necessary and all changes must also be approved by the Board of Directors.	- Inquire of the Corporate Security Officer to determine the process for updating the Acceptable Use Policy document and obtaining appropriate approvals from management. - Inspect the most recently approved Initech Acceptable Use Policy to determine that the most recent version had changes logged and was it appropriately approved by management. - Inspect the most recent annual approval for the current fiscal year from the Board of Directors to determine that it was completed within the last 12 months.
	CO-AUP-1-CA2 - The Initech Acceptable Use Policy document is made available to all employees and to new employees at the time of joining. An acknowledgement is required from each employee on an annual basis and within 30 days of joining to assert that they have read and agree with terms of the Acceptable Use Policy.	- Inquire of Corporate HR and Compliance Manager to understand the process for distributing the Acceptable Use Policy and obtaining acknowledgement of the employees on an annual basis and when new employees join. - Inspect the new hire checklist to determine that new hires are required to complete Acceptable Use Policy Training and acknowledgment as part of onboarding. - Inspect a sample of 25 new hires to determine that they have acknowledged the Initech Acceptable Use Policy - Inquire of 50 personnel to determine if the policy has been actively disseminated and is readily available to those expected to comply. Refer to **CO-AUP-4** for additional testing related to Awareness and Training of the Acceptable Use Policy.
CO-AUP-2 - Controls are in place to prevent inappropriate use of Initech systems and data.	**CO-AUP-2-CA1** - A website/e-mail filtering tool is in place to monitor and prevent inappropriate websites and block emails based on inappropriate attachments and mail contents. The tool also monitors employee activities and usage trends and blocks access after a certain period of time.	- Inquire of the Corporate Security Officer to determine the controls in place to monitor website and email usage and block inappropriate activities. - Inspect Palo Alto web filtering rules to determine that inappropriate site categories and sites are blocked by default. - Inspect a sample of 25 employee workstations or laptops (from 5 different departments and separate job roles) to determine if inappropriate websites are blocked. - Inspect Palo Alto web filtering logs to determine that inappropriate access is logged in the ticketing system for Corporate Security to investigate. Refer to **CO-AUP-5** for additional testing related to Initech Corporate Security response and investigation related to Unacceptable Use.
	CO-AUP-2-CA2 - External endpoint devices such as USB and CD/DVD drives are blocked by default in workstations or laptops. Employees can gain access to the external devices after proper approval. A script is run on a daily basis to deactivate external devices that were approved for temporary exception.	- Inquire of the Corporate Security Officer to determine the controls in place to prevent use of external endpoint devices and obtain approval for exceptions. - Inspect a sample of 25 employee workstations or laptops (from 5 different departments and separate job roles) to determine if external USB devices are blocked. - Inspect the external devices enabled systems to determine if manager approval was obtained within last six months. - Inspect the script that runs each day to confirm that it blocks USB access for employees that have expired their six month exceptions.
	CO-AUP-2-CA3 - The Information security group regularly monitors and maintains least privilege access for all the employees. Employees have been given the minimum access that is necessary for them to perform day to day job responsibilities. Based on proper authorization, local workstation admin access can only be granted to an employees workstation with manager approval. Approvals are valid for three months and must be reapproved to maintain the admin access.	- Inquire of the Corporate Security Officer to determine the controls in place to limit local admin access to appropriate personnel and obtain approval for elevated privileges. - Inspect a sample of 25 employee workstations or laptops (from 5 different departments and separate job roles) to determine if local admin access is restricted. - Inspect the systems with admin rights to determine if manager approval was obtained within last three months.
CO-AUP-3 - Controls are in place to detect inappropriate use of Initech systems and data.	**CO-AUP-3-CA1** - Initech Corporate Security defines the criteria for applications and systems to be monitored and events to be logged. The Enterprise Security Incident Management (SIEM) system will correlate logs and alert on potential inappropriate activity that require logged in the Initech Ticket System and investigated by Initech Security.	- Inquire of the Corporate Security Officer to determine the criteria for applications and systems to be monitored and logged. - Inspect a sample of 25 servers to determine each server is sending user activity logs to the Enterprise SIEM. - Inspect the configuration of the Enterprise SIEM alerts to determine if they are designed to detect unacceptable use of Initech Systems - Inspect a sample of 25 SIEM alerts to determine that all alerts were logged in the Initech Ticket System to be investigated by Initech Security. Refer to **CO-AUP-5** for additional testing related to Initech Corporate Security response and investigation related to Unacceptable Use.

Initech Acceptable Use Policy
Audit Plan

Sherlock Group
December 2015

Control Objective	Control Activities	Audit Procedures
	CO-AUP-3-CA2 - The Initech Social Media Department monitors all major Social Media platforms to ensure appropriate use of Social Media at Initech. Incidents of inappropriate use are logged in the Initech Ticket System and investigated by Initech Security.	- Inquire of the Social Media Compliance Manager to determine the procedures for monitoring Social Media activity and responding to inappropriate use. - Perform data analytics of major Social Media platforms (e.g. Facebook, Twitter, and LinkedIn) to identify potential unacceptable use by Initech employees (i.e. posts that tarnish the image of Initech or its employees) - Inspect a sample of inappropriate Social Media posts to determine that they were logged in the Initech Ticket system and investigated by Corporate Security. Refer to **CO-AUP-5** for additional testing related to Initech Corporate Security response and investigation related to Unacceptable Use.
	CO-AUP-3-CA3 - Initech Corporate Security defines DLP rules for monitoring data transmissions over enabled external media devices (e.g. open USB ports) and email. DLP alerts are generated for potential inappropriate use and are logged in the Initech Ticket System and investigated by Corporate Security.	- Inquire of the Corporate Security Officer to determine the DLP rules in place to monitor data transmissions and the process for investigating DLP alerts. - Inspect the Initech Data Classification Policy to determine the data that is considered sensitive at Initech. - Inspect a listing of the DLP rules to determine that they adequately monitor sensitive data (as defined by the Initech Data Classification Policy). - Observe attempts to move "mock" sensitive data via an open USB port and e-mail to confirm that the rules are appropriately configured and create alerts for investigation. - Inspect a sample of 25 DLP alerts of previously logged incidents to determine that they were logged in the Initech Ticket system and investigated by Corporate Security. Refer to **CO-AUP-5** for additional testing related to Initech Corporate Security response and investigation related to Unacceptable Use.
CO-AUP-4 - Controls are in place to ensure appropriate awareness and training of the Acceptable Use Policy.	**CO-AUP-4-CA1** - The Enterprise Security Learning Management System (SLMS) includes a course that requires all employees to complete Acceptable Use Policy training on an annual basis. The system will issue certificates for employees that have completed the training, passed the comprehension test, and have acknowledged their understanding of the policy.	- Inquire of the Compliance Manager to determine the process for employees to complete the Acceptable Use Policy training on an annual basis. - Inspect the Enterprise SLMS Acceptable Use Policy course to determine if the training given to the employees aligns with the Initech Acceptable Use Policy. - Inspect a sample of 50 employees for validation of training completion and issuance of certificates by the Enterprise SLMS.
	CO-AUP-4-CA2 - The Enterprise SLMS will simulate mock phishing emails within 3 weeks after employees have completed Acceptable Use Training. All incidents of failed phishing testing is logged in the Initech Ticket System and investigated by Initech Security.	- Inquire of the Corporate Security Officer to determine the process for conducting simulated phishing e-mail training and following-up with individuals that inappropriately open simulated phishing attempts. - Observe an attempt to open a simulated phishing e-mail to determine that it logs a ticket in the Initech Ticket System and is routed to Initech Security for investigation. - Inspect a sample of 25 failed phishing simulations to determine that they were logged in the Initech Ticket System and investigated by Initech Security.
	CO-AUP-4-CA3 - The Enterprise SLMS will alert People Managers of employees that have not successfully completed the Acceptable Use Policy on an annual basis. People Managers must follow-up with employees to ensure they complete their training.	- Inquire of the Compliance Manager to determine the escalation process for incomplete Acceptable Use Policy training. - Inspect a sample of past due trainings to determine that Human Resource Department was notified. - Inspect a sample of 25 employees that have not completed the Initech Acceptable Use Policy and observe evidence that employees were escalated for past due training.
CO-AUP-5 - Controls are in place to respond to inappropriate use at the organization.	**CO-AUP-5-CA1** - Corporate Security defines the criteria for assigning a severity to all tickets that require investigation and response. The tickets sent to Corporate Security are each assigned the appropriate severity when they are received.	- Inquire of the Corporate Security Officer to determine the process for assigning severity levels to all tickets associated with Unacceptable Use. - Inspect the Corporate Security policy to determine that the criteria for each security severity level is clearly defined. - Inspect a sample of 25 Security tickets to determine that they were assigned the appropriate severity level.

Initech Acceptable Use Policy
Audit Plan

Sherlock Group
December 2015

Control Objective	Control Activities	Audit Procedures
	CO-AUP-5-CA2 - Corporate Security has SLAs established to investigate security incidents logged in the Initech Ticket System within a reasonable period of time.	- Inquire of the Corporate Security Officer to determine the SLAs defined for investigating all tickets associated with Unacceptable Use. - Inspect the security incident SLAs within the Corporate Security policy to determine whether appropriate response time is defined for each severity level. - Inspect a sample of 25 tickets from the Initech Ticket System to determine that they were investigated in accordance to the SLA.
	CO-AUP-5-CA3 - Corporate Security policy requires repeat offenders of inappropriate use to be communicated to HR for appropriate actions.	- Inquire of the Corporate Security Officer to understand the process of communicating repeat offenders to HR. - Perform data analytics on the full population of previous tickets to identify repeat offenders and determine if repeat offenders are referred to HR.