2020

Assignment 4

ISEC3800

POD 7 – COURTNEY HAGEN, JESSEY HARLOW, ZACH SLAUNWHITE

Table of Contents

Assignment 4

Introduction

This assignment is intended to aid us in learning how to write policies for companies we may work for when we're sent to industry. NSCC templates are given to help structure the policies. With the completion of this assignment, we should be able to write a simple policy pertaining to IT related topics.

Technology Equipment Disposal Policy

Overview

Technology disposal can affect a company negatively via public perception, lost revenue, and legal action if not done properly. The Technology Equipment Disposal Policy is set to eliminate confusion as to handle the disposal of technology equipment so that these negative impacts can be avoided.

Purpose

The purpose of this policy is to outline how to handle NSCC's Institute of Technology campus' technology equipment when the equipment is to be disposed of.

Scope

This policy covers any technology equipment that has determined to no longer hold value or use to NSCC, specifically, the Institute of Technology campus. All employees at NSCC's Institute of Technology campus must follow this policy to ensure proper disposal of technology equipment.

Policy

Technology Equipment Definition

Technology equipment includes any networking equipment, computers, telephony, or computer peripherals. Computers include desktops, laptops, and servers. Computer peripherals include but are not limited to printers, monitors, keyboards, mice, microphones, cameras, batteries, USB media, and any other equipment used with the IT infrastructure. Networking equipment includes but is not limited to routers, switches, and cabling. Telephony includes any landline, IP, or mobile phone devices and peripherals.

Technology Equipment Disposal Team

The Technology Equipment Disposal Team will be responsible for executing this policy. All technology equipment to be disposed must be brought to the Technology Equipment Disposal Team in some fashion to dispose of according to this policy.

When to Dispose

Equipment is only to be disposed of when it no longer holds value or use to the company. The Technology Equipment Disposal Team will have the final say as to what should be disposed of.

Technology Equipment Disposal

Data

Any type of storage medium in any device will be securely wiped and physically destroyed so that any data is completely unrecoverable.

Recycling

All technology equipment will be sent to a recycling facility. Technology equipment will not be trashed or sent to a landfill. Recycling locations will be set throughout the Campus for the Technology Equipment Disposal Team to proceed to properly recycle according to provincial regulations.

Working Equipment

Any equipment which has deemed no longer useful to NSCC will be collected and auctioned off. The proceeds will be given to the NSCC Foundation.
Any equipment that has parts that remain useful to NSCC will have those parts removed and repurposed. The rest of that device that is no longer useful will be recycled.

Compliance

Compliance will be measured by upkeeping the asset tracking register. A member of the Technology Equipment Disposal will be responsible to sign off on their recycling of the equipment they have recycled.
Management reserves the right to discipline any employee who does not abide by this policy. Any employee found violating the law surrounding taking company equipment and proper sensitive data disposable may also be held legally accountable.

Data Center Access

Overview

The data center has a lot of valuable hardware, all running business critical processes on it, there needs to be rules and regulations on access and usage.

Purpose

This policy is meant to govern who can have access to the data center, when they're able to access it, who they're able to give temporary access to, what they're allowed to do in the data center, and how broken rules regarding this policy are dealt with.

Scope

The scope of this policy covers visitors, students, staff and their usage of the data center.

Policy

Visitors

Visitors are under no circumstances allowed within the data center without signing, and without being guided by a staff member. Students are not allowed to accompany guests, and only approved staff can accompany guests. Guests may not touch any running production equipment, but they're free to handle anything not in use, with direction from the staff member guiding them.

Staff

All staff members must sign in on the staff sign in and out sheet when they enter and exit the data center. Only the pre-approved data center employees are allowed to sign in on this sheet, any other staff will be treated similar to guests, and will have to sign in on the guest sign in page, and must be guided by one of the approved data center employees. Not approved staff may not handle any production equipment but can handle non-production equipment with the direction of an approved

employee. Approved employees can access the data center any time, but outside of business hours must provide a written reason as to why they're accessing the center outside of normal operating hours.

Students

Students must sign in with the student sign in sheet, as well as describe their reasoning for using the data center equipment. Students may only be in the data center while an approved employee is present, but doesn't need to be guided, as long as they've gone through the initial seminar on what they're able to and not able to do within the data center. Students are only allowed to handle live production equipment under the direction and supervision of an approved employee but can handle student data center equipment whenever they wish, if they're doing instructor approved work.

Open Door Times

The door is open to all IT students from 10AM until 3PM, if an approved employee is present. Anyone else needs to request access, and be guided by an approved employee, aside from approved employees.

Usage

Approved employees are only able to do task approved by their manager or director. Visitors may not use any equipment. Students are only able to use production equipment if approved by approved employees but may use student data center hardware if approved by an instructor and an approved employee.

Compliance

The punishment for non-approved access depends on the severity of actions taken within the data center. If someone who has not been approved uses the data center, they will be kicked out of the data center for one week, indefinitely, or indefinitely with police intervention. If someone accesses the data center with no approval but touches nothing, they will lose access for one week. If someone accesses the data center, and tampers with equipment, but doesn't injure the production environment or steal anything they lose access indefinitely. If someone accesses the data center and injures the production environment or steals something, they lose access indefinitely, police intervention will be used, and they will risk being kicked out of the school, fired, or black listed, depending on what kind of visitor they are.

Remote Access Policy

Overview

Remote access is used only when necessary, in most cases students are able to make it to campus to use the computers after hours or during business hours, and only when the school is closed, limiting usage during normal hours will remote access be given, outside of employees.

Purpose

The purpose of this policy is to limit remote access, and to govern when and how someone may use equipment in the school with remote access.

Scope

The scope of this policy is for anyone that figures out how to get access to remote access, or any students,

Policy

General Employee

General employees are given the ability to remote access into their working machines but must provide a reason as to why they need to use it outside of business hours.

IT Employees

IT employees are granted remote access to their working machines, and any servers they may need to access at home in case of emergency, no reasons need to be provided if system logging is set on.

Student

Students will have remote access set up on their workstations but will only be given guidelines on how to use it in case of campus restriction.

Compliance

If remote access is used without being given permission, or with permission but for malicious activities, depending on the usage the following will apply. If remote access is used without permission, but not for malicious activities, the user may be punished with loss of remote access and a strike on their employee or student record. If remote access is used for malicious activity users will be punished by being fired or expelled and depending on the activity police intervention will be applied.

Email/Communication Policy

Overview

Email is something every student and employee is given, and anyone that visits the public library is given access to email on the computers as well. The school may be held liable for any malicious acts taken over email.

Purpose

This policy is meant to oversee usage and access to email on campus, or with school domain emails.

Scope

The scope of this policy is any student or employee given an email through the college with the domain name nscc.ca or campus.nscc.ca. The scope also covers anyone using personal emails in the school library, that's open to the public.

Policy

Employees

Employees may only use the school given emails for work related activities, and do not have permission to use them to sign up for any promotions, or services. Employees aren't given permission to email anyone for personal reasons using this email either, it is to be used strictly for work related purposes.

Students

Students may only use the school given emails for school related activities, and do not have permission to use them to sign up for any promotions, or services unless given permission, or required by an instructor for work purposes. Students aren't given permission to email anyone for personal reasons

using this email either, it is to be used strictly for work school purposes. Special circumstances that are fine are using the email to speak with potential coop or work term employers, and for professional networking websites like LinkedIn.

Visitors

Visitors are not given a NSCC domain email, so the rules around usage for that do not apply. Visitors are free to use their personal email on campus in any way they see fit, as long as it doesn't conflict with provincial, or federal law in any way.

Compliance

If students use their emails in ways NSCC does not approve they may lose their provided domain email. If staff use their staff email in a way NSCC does not approve they will either receive a strike, or lose their job depending on the amount of times notified. If anyone uses their provided email, or personal email on campus in a way that conflicts with provincial or federal law, the authorities will be notified, and the situation will be handled by them. If authorities are involved, the employee will lose their job, and a student will be expelled.

General Employees Confidentiality Policy

Overview

Confidentiality in a company carries ethical, business related, and legal ramifications if not taken seriously. This General Employees Confidentiality Policy is set to protect NSCC's Institute of Technology's confidential information.

Purpose

The purpose of this policy is to outline safeguards for maintaining confidential information and what qualifies as breaking confidentiality.

Scope

This policy covers all general employees at the NSCC Institute of Technology campus excluding executive members, department heads, HR employees, and IT employees who have specific confidentiality policies.

Policy

Confidential Information Definition

Confidential information includes any data entrusted to us by our students, staff, industry partners, and any other individual or organization that interacts with our company. This includes but is not limited to internal documents, student information, accounting information, staff information, proprietary information, unpublished information, documents marked as confidential, etc.

Safeguards for Confidential Information

Confidential information should have physical security. This includes paper documents being kept locked away when not in use, and shredded when they are no longer needed. In terms of digital security, these documents should only be used on company devices by those authorized to do so. All machines should be locked upon leaving them, and those documents should not be opened when not in use. Any machine used to access sensitive information should be in an office and able to be locked away, (in the

case of a laptop). If a laptop is needed to be taken out of the office with sensitive information, this machine will be encrypted and must be locked away when not in use. It may not be left in high theft areas such as left in a car.

Breaking Confidentiality

The following are things employees cannot do regarding confidentiality and confidential information:

- Employees should not discuss confidential information to anyone who is not authorized to know this information and does not need to know this information. This includes people outside of the company as well as people inside of the company who this information was not meant for.
- Employees should not copy confidential information on personal devices or devices not intended to access this confidential information.
- Employees should not personally benefit or profit from confidential information.

Doing any of these actions would be considered breaking confidentiality.

Compliance

Breaking confidentiality and not following safeguards for confidential information may result in discipline up to termination. Management reserves the right to decide the discipline based on the impact of the action. Legal action may be taken if one is found breaking confidentiality or not following safeguards for confidential information if doing so violates provincial or federal law.

Executive Members and Department Heads Confidentiality Policy

Overview

Confidentiality in a company carries ethical, business related, and legal ramifications if not taken seriously. This Executive Members and Department Heads Confidentiality Policy is set to protect NSCC's Institute of Technology's confidential information.

Purpose

The purpose of this policy is to outline safeguards for maintaining confidential information and what qualifies as breaking confidentiality in a management role.

Scope

This policy covers all Executive Members and Department Heads at the NSCC Institute of Technology campus. Separate policies will cover general employees, human resource employees, and IT department employees.

Policy

Confidential Information Definition

Confidential information includes any data entrusted to us by our students, staff, industry partners, and any other individual or organization that interacts with our company. This includes but is not limited to internal documents, student information, accounting information, staff information, proprietary information, unpublished information, documents marked as confidential, etc.

Safeguards for Confidential Information

Confidential information should have physical security. This includes paper documents being kept locked away when not in use, and shredded when they are no longer needed. As an Executive member or department head, there is a stronger need for locking the door to your office when the room is left, and not leaving paper visible when there are visitors in the room. In terms of digital security, these documents should only be used on company devices by those authorized to do so. All machines should be locked upon leaving them, and those documents should not be opened when not in use. Any machine used to access sensitive information should be in an office and able to be locked away, (in the case of a laptop). If a laptop is needed to be taken out of the office with sensitive information, this machine will be encrypted and must be locked away when not in use. It may not be left in high theft areas such as left in a car.

Breaking Confidentiality

The following are things employees cannot do regarding confidentiality and confidential information:

- Executive members and department heads should not discuss confidential information to anyone who is not authorized to know this information and does not need to know this information. This includes people outside of the company as well as people inside of the company who this information was not meant for.
- Executive members and department heads should not copy confidential information on personal devices or devices not intended to access this confidential information.
- Executive members and department heads should not personally benefit or profit from confidential or privileged information.

Doing any of these actions without written consent would be considered breaking confidentiality.

Compliance

Breaking confidentiality and not following safeguards for confidential information may result in discipline up to termination. Management reserves the right to decide the discipline based on the impact of the action. Legal action may be taken if one is found breaking confidentiality or not following safeguards for confidential information if doing so violates provincial or federal law.

HR Department Employees Confidentiality Policy

Overview

Confidentiality in a company carries ethical, business related, and legal ramifications if not taken seriously. This Human Resources Department Employees Confidentiality Policy is set to protect NSCC's Institute of Technology's confidential information as well as the personal and sensitive information of students and staff.

Purpose

The purpose of this policy is to outline safeguards for maintaining confidential information and what qualifies as breaking confidentiality.

Scope

This policy covers all HR Department employees at the NSCC Institute of Technology campus. Separate policies will cover general employees, IT department employees, and executives and department heads.

Policy

Confidential Information Definition

Confidential information includes any information unintentionally overhead, or any data entrusted to us by our students, staff, industry partners, and any other individual or organization that interacts with our company. This includes but is not limited to internal documents, student information, accounting information, staff information, proprietary information, unpublished information, documents marked as confidential, etc.

Safeguards for Confidential Information

Meetings and discussions involving confidential and privileged information will be conducted behind closed doors in a designated room. Confidential and privileged information will not be discussed outside of the office to avoid any information from being overheard. Confidential information should have physical security. This includes paper documents being kept locked away when not in use, and shredded when they are no longer needed. In terms of digital security, these documents should only be used on company devices by those authorized to do so. All machines should be locked upon leaving them, and those documents should not be opened when not in use. Any machine used to access sensitive information should be in an office and able to be locked away, (in the case of a laptop). If a laptop is needed to be taken out of the office with sensitive information, this machine will be encrypted and must be locked away when not in use. It may not be left in high theft areas such as left in a car.

Breaking Confidentiality

The following are things employees cannot do regarding confidentiality and confidential information:

- HR employees should not discuss confidential information to anyone who is not authorized to know this information and does not need to know this information. This includes people outside of the company as well as people inside of the company who this information was not meant for.
- HR employees should not copy confidential information on personal devices or devices not intended to access this confidential information.
- HR employees should not personally benefit or profit from confidential information.
- HR employees should not look up sensitive information of any staff or student unless the information is relevant to the duties of HR.

Doing any of these actions without written consent would be considered breaking confidentiality.

Compliance

Breaking confidentiality and not following safeguards for confidential information may result in discipline up to termination. Management reserves the right to decide the discipline based on the impact of the action. Legal action may be taken if one is found breaking confidentiality or not following safeguards for confidential information if doing so violates provincial or federal law.

IT Department Employees Confidentiality Policy

Overview

Confidentiality in a company carries ethical, business related, and legal ramifications if not taken seriously. This IT Department Employees Confidentiality Policy is set to protect NSCC's Institute of Technology's confidential information.

Purpose

The purpose of this policy is to outline safeguards for maintaining confidential information and what qualifies as breaking confidentiality.

Scope

This policy covers all IT department employees at the NSCC Institute of Technology campus. Separate policies will cover general employees, human resource employees, and executive members and department heads.

Policy

Confidential Information Definition

Confidential information includes any information unintentionally overhead, or any data entrusted to us by our students, staff, industry partners, and any other individual or organization that interacts with our company. This includes but is not limited to internal documents, student information, accounting information, staff information, proprietary information, unpublished information, documents marked as confidential, etc.

Safeguards for Confidential Information

Confidential information should have physical security. This includes paper documents being kept locked away when not in use, and shredded when they are no longer needed. In terms of digital security, these documents should only be used on company devices by those authorized to do so. All machines should be locked upon leaving them, and those documents should not be opened when not in use. Any machine used to access sensitive information should be in an office and able to be locked away, (in the case of a laptop). If a laptop is needed to be taken out of the office with sensitive information, this machine will be encrypted and must be locked away when not in use. It may not be left in high theft areas such as left in a car.

Breaking Confidentiality

The following are things employees cannot do regarding confidentiality and confidential information:

- IT Employees should not discuss confidential information to anyone who is not authorized to know this information and does not need to know this information. This includes people outside of the company as well as people inside of the company who this information was not meant for.
- IT Employees should not copy confidential information on personal devices or devices not intended to access this confidential information.
- IT Employees should not personally benefit or profit from confidential information.
- IT Employees should not use their elevated roles to research sensitive information that does not pertain to the responsibilities of IT.

Doing any of these actions without written consent would be considered breaking confidentiality.

Compliance

Breaking confidentiality and not following safeguards for confidential information may result in discipline up to termination. Management reserves the right to decide the discipline based on the impact of the action. Legal action may be taken if one is found breaking confidentiality or not following safeguards for confidential information if doing so violates provincial or federal law.

References

Technology Equipment Disposal Policy. (2014, June). Retrieved April 7, 2020, from https://www.sans.org/security-resources/policies/server-security/pdf/technology-equipment-disposal-policy

Employee Confidentiality Policy Template. (2020, March 12). Retrieved April 8, 2020, from https://resources.workable.com/confidentiality-company-policy