**ITS1103 Ethics & Information Technology**

**IT Equipment Usage and Abuse Prevention** **Guidelines and Policies**

This paper on Guidelines provides a comprehensive overview of how organizations can maintain secure, ethical, and productive workplaces. Its main objective is to outline policies that protect company assets, prevent cyber-attacks, and ensure employee compliance with legal and ethical standards. Key areas include preventing Denial of Service attacks, proper software and email usage, implementing strong cybersecurity measures like MFA, regular backups, and monitoring for suspicious activity. The guidelines also emphasize ethical decision-making in software development, data privacy, intellectual property compliance, and workplace monitoring.

This work is valuable for cybersecurity because it demonstrates an understanding of policy-based risk management and proactive threat prevention. These are indispensable skills for protecting organizational systems. It also highlights the practical implementation of security measures, from phishing awareness training to software licensing compliance, which directly relate to cybersecurity responsibilities.

The relevance to cybersecurity work is further reinforced through the detailed discussion of monitoring, reporting, and remediation procedures, as well as compliance with standards like GDPR and HIPAA. By addressing both human behavior and technical controls, this paper reflects critical skills in risk assessment, policy enforcement, and ethical decision-making, all of which are necessary for effective cybersecurity management and maintaining a secure organizational environment.

**Week 5 Compilation**

**Anna Kephart**

**ITS1103 Ethics & Information Technology**

**August 12, 2024**

**Code of Computer Conduct and Ethics for Ajax Digital Information (ADI)**

**Purpose Statement:**

These guidelines establish a framework for responsible and secure use of IT resources by employees at Ajax Digital Information (ADI). By outlining the core principles, safeguarding against misuse, and promoting ethical conduct, these guidelines ensure both organizational integrity and the well-being of our workforce.

Table of Content

***IT Equipment Usage and Abuse Prevention Guidelines***

* ***Addressing Denial of Service***
* ***Mitigating Cyberattacks and Cybersecurity***
* ***Ethical Decisions in Software Development***

***Comprehensive Data Privacy and IT Usage Policy***

* ***Introduction***
* ***Data Privacy Policy***
* ***Corporate IT Usage Policy***
* ***Internet Access***
* ***Content Restrictions***
* ***Reporting and Compliance***
* ***Legal Measures***

***Internet and Email Usage Policy***

* ***Accessing Content from the Internet***
* ***Email Communication***
* ***Protection Against Viruses and Malware***

***Social Media Code of Conduct***

* ***Transparency and Disclaimers***
* ***Conduct Guidelines***
* ***Posting about Competition***
* ***Branding and Product Communication***
* ***Handling Negative Content***
* ***Responding to Complaints***
* ***Privacy Protection***
* ***Disciplinary Actions***

***Contingent Worker Policy***

* ***Definition ad Benefits***
* ***Assignment Management***
* ***Legal Awareness***
* ***Job Requirements and Equipment***
* ***Training and Supervision***
* ***Leasing Firm Responsibilities***

**Intellectual Property - Copyright**

* **Usage of Licensed Software**
* **Shareware Policies**
* **Software Piracy Rule and Consequences**

**Privacy**

* **Secure Communications**
* **Data Surveillance**
* **Protecting Privacy**

***IT Equipment Usage and Abuse Prevention Guidelines***

These guidelines outline the responsible and secure use of company equipment. All users are expected to adhere to these rules to maintain the integrity and efficiency of our systems. Failure to comply may result in disciplinary action, including termination.

*Addressing Denial of Service:*

*Denial of Service (DoS) incidents can occur accidentally or intentionally, leading to disruptions within the organization. To prevent DoS, users must follow these guidelines:*

1. ***Network Usage Awareness:***

* Users should be mindful of their network activity. Excessive bandwidth usage during working hours can impact other users.
* Large file transfers should be approved by managers to avoid network congestion.
* Requests for additional hardware systems should be submitted through proper channels.

1. ***Software Usage:***

* Users are not authorized to install or use software that hasn’t been approved by the IT system administrator.
* Personal file storage on company computers is strictly prohibited.

1. ***Email Management:***

* Regularly maintain email storage to prevent system shutdowns.
* Keep email accounts organized and up to date.

***Mitigating Cyberattacks and Cybersecurity***

1. ***Prevention***

* All employees are required to participate in yearly cybersecurity training to stay informed on the latest threats and best practices.
* All employees are required to participate in Phishing, Smishing and Vishing Awareness Training regularly. Employees should report any suspicious email, text, or voicemail activity. (Ethics in Information Technology)
* All employees are required to participate in all social engineering training provided by the company.
* All employees are required to comply with company policies to use strong and unique passwords. These passwords will need to be changed every 90 days to prevent attacks.
* Enable MFA (Multi Factor Authentication) for all hardware where company accounts are logged in.
* Ensure your data is backed up regularly. (Heimdal Security, n.d.)
* Employees are required to keep all organization hardware up to date with all updates
* Firewall and Antivirus Software is installed on all employees' laptops; employees are prohibited from changing any Firewalls or Antivirus software. (SecurityScorecard, n.d.)

1. ***Detection***

* Employees are required to report any suspected harmful activities to the IT Department
* Employees are required to get training and be aware of how to report any incidents that may affect the organization's data.

1. ***Remediation***

* Employees are required to report any suspicious activity of unauthorized application installation to the IT department
* Employees are required to report any suspicious activity of unauthorized usage of data to the IT department
* Employees are required to report any suspicious activity of unauthorized hardware usage to the IT department

***Ethical Decisions in Software Development***

1. ***Privacy and Data Protection***

* Employees are reminded to be ethical and respect user privacy
* Employees are reminded to be aware of unethical and unauthorized data collection (Institute Data, n.d.)

1. ***Consent***

* Always inform customers of data collection and usage; including any third-party vendors

1. ***Quality Assurance***

* Deliver high quality software that meets the needs of the customers and ensures ethical standards are met.
* Deliver thoroughly tested software with any knows bugs fixed to ensure customer satisfaction. (Ethics in Information Technology)

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

### **Comprehensive Data Privacy and IT Usage Policy**

**1. Introduction:**

* Ajax Digital Information is committed to protecting the privacy and security of personal and corporate data. This policy outlines our approach to data privacy and the acceptable use of IT resources.

**2. Data Privacy Policy:**

* **Purpose:** To ensure the confidentiality, integrity, and availability of data.
* **Scope:** Applies to all employees, contractors, and third-party service providers.
* **Data Handling:** Personal and corporate data must be handled in accordance with applicable laws and regulations.
* **Data Storage:** Data must be stored securely, with access restricted to authorized personnel only.
* **Data Sharing:** Data sharing is limited to what is necessary for business operations and must be done securely.
* **Data Breach:** Any data breach must be reported immediately to the Data Protection Officer.

**3. Corporate IT Usage Policy:**

* **Network Capacity:** Employees must conserve corporate network capacity by limiting nonbusiness use of information resources.
* **Legal Liability:** Employees must avoid actions that could result in legal liability for the company.
* **Productivity:** Nonbusiness use of IT resources should be minimized to improve worker productivity.

**4. Internet Access:**

* **Nonbusiness Websites:** Access to nonbusiness-related websites is restricted through Internet filters, firewall configurations, and the use of ISPs that block such sites.
* **Anonymous Remailers:** The use of anonymous remailers is prohibited and monitored by our corporate firewall.

**5. Content Restrictions:**

* **Defamation and Hate Speech:** Defamation and hate speech are strictly prohibited in the business setting.
* **Pornography:** Viewing and sending pornographic material is prohibited.
* **Monitoring:** Employee email is regularly monitored for defamatory, hateful, and pornographic content.

**6. Reporting and Compliance:**

* **Incident Reporting:** Employees must report any receipt of hate mail or pornography to HR immediately.
* **Anonymous Complaints:** HR will handle complaints anonymously and confidentially.
* **Compliance Monitoring:** Compliance will be monitored through computer logs and security systems.

**7. Legal Measures:**

* **John Doe Lawsuits:** In cooperation with legal counsel, the company has a policy on the use of John Doe lawsuits to identify authors of libelous, anonymous emails.

### **Internet and Email Usage Policy**

**1. Accessing Content from the Internet:**

* Employees must use the Internet primarily for business purposes.
* Employees should avoid accessing websites that could compromise network security or productivity.

***2. Email Communication:***

* Email should be used primarily for business communication.
* Employees must avoid sending or receiving defamatory, hateful, or pornographic material.
* Employee email is regularly monitored to ensure compliance with company policies.

**3. Protection Against Viruses and Malware:**

* Employees must use company-approved antivirus software and ensure it is regularly updated.
* Employees should avoid downloading or opening attachments from unknown or suspicious sources.
* Any suspected malware or virus activity must be reported immediately to the IT department.

By adhering to this comprehensive policy, Ajax Digital Information aims to maintain a secure, productive, and respectful workplace for all employees.

### **Social Media Code of Conduct**

**1. Transparency and Disclaimers:**

* Employees must include an “opinions are my own” disclaimer on their social media profiles.
* Employees must clearly state that they work at Ajax Digital Information in their social media profiles.

**2. Conduct Guidelines:**

* Employees are advised to act respectfully and be part of the solution, not part of the problem.
* Confidentiality must be maintained regarding unannounced product releases, company financial data, and nonpublic company news.

**3. Posting About Competition:**

* Employees should behave diplomatically, ensure they have the facts straight, and obtain appropriate permissions when posting about competitors.

**4. Branding and Product Communication:**

* Guidance is provided on what customers can expect from our products and how they differ from the competition.
* Employees are instructed on how to talk about specific products accurately and positively.

**5. Handling Negative Content:**

* Employees are advised on how to react if they see negative content regarding our brand, including reporting it to the appropriate department.
* Employees must credit original sources when reposting or posting copyrighted material.

**6. Responding to Complaints:**

* Practical advice is given on how to respond to complaints respectfully and tactfully.

**7. Privacy Protection:**

* The policy addresses the need to protect the personal privacy of both customers and employees.

**8. Disciplinary Actions:**

* It is clearly stated that disciplinary action, up to and including termination, will be taken if employees do not follow these guidelines.

### **Contingent Worker Policy**

**1. Definition and Benefits:**

* The definition of an employee in our company’s policies and pension plan documents has been reviewed to ensure it does not encompass contingent workers, thus entitling them to benefits.

**2. Assignment Management:**

* We are careful not to use the same contingent workers on an extended basis and ensure assignments are finite, with break periods in between.
* Contracts specifically designate workers as contingent workers.

**3. Legal Awareness:**

* We are aware that the actual circumstances of the working relationship determine whether a worker is considered an employee in various contexts, and that our definition of a contingent worker may not be accepted as accurate by a government agency or court.
* Managers and workers are aware that staffing firm employees are covered by antidiscrimination laws and cannot be discriminated against based on race, color, religion, sex, national origin, or disability.

**4. Job Requirements and Equipment:**

* We avoid telling contingent workers where, when, and how to do their jobs, and instead work through the contingent worker’s manager to communicate job requirements.
* Contingent workers are requested to use their own equipment and resources, such as computers and email accounts.

**5. Training and Supervision:**

* We avoid training contingent workers.
* When leasing employees from an agency, we let the agency do its job and avoid asking to see résumés, getting involved with compensation, performance feedback, counseling, or day-to-day supervision.

**6. Leasing Firm Responsibilities:**

* If we lease employees, we use a leasing firm that offers its own benefits plan, deducts payroll taxes, and provides required insurance.

By adhering to these policies, Ajax Digital Information ensures a respectful, compliant, and productive work environment for all employees and contingent workers.

**Business Plan for Code of Conduct Training**

**Objective:** To ensure all employees of Ajax Digital Information are thoroughly trained and certified in the company’s Code of Conduct, fostering a culture of ethical behavior and compliance.

**Implementation Plan:**

1. **Training Delivery:**

* Department managers will conduct formal training sessions.
* Training material will be reviewed, quizzed, and certified for each employee.
* The training will be comprehensive, covering the manual section by section.

1. **Training Schedule:**

* Mandatory training will be completed within three months, providing ample time for all employees.
* Annual training sessions will be scheduled to ensure ongoing compliance and understanding.

**Timeline:**

* **Month 1:**
* Managers will send out email communications to inform employees about the mandatory training.
* Training sessions will be organized and scheduled by department managers.
* **Months 2-3:**
* Managers will conduct training sessions, ensuring all employees complete the training.
* Employees will sign the Code of Conduct to acknowledge their understanding and compliance.

**Compliance Monitoring:**

* Compliance will be tracked through computer logs and security systems.
* The HR department will handle complaints, ensuring anonymity and confidentiality.
* Complaints can be submitted via email, letter, or verbal communication during meetings, at any time.

By implementing this structured training plan, Ajax Digital Information aims to uphold the highest standards of ethical behavior and ensure all employees are well-versed in the company’s Code of Conduct.

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**Intellectual Property – Copyright**

**Copyright** is a type of intellectual property that grants the creator of an original work exclusive rights to its use and distribution. This means the creator can control how the work is used, reproduced, and distributed.

**Usage of Licensed Software**

* **Licensed Software**: Only use licensed software purchased by the company for work purposes. Using it elsewhere is prohibited and may result in disciplinary action or termination.
* **Compliance with Licensing Agreements:** Ensure all software used within the company is properly licensed. This includes understanding and complying with the terms of End-User License Agreements (EULAs) which typically prohibit copying, modifying, or sharing software.
* **Software Asset Management (SAM):** Here at Ajax Digital Information, we use SAM tools to track and manage software licenses, ensuring that all software installations are legitimate and up to date.
* **Regular Audits:** We perform regular internal audits to ensure compliance with software licensing agreements and to identify any unauthorized software.
* **Employee Education:** Conduct regular training sessions to educate employees about the importance of software licensing and the legal and ethical implications of software piracy.

**Shareware Policies**

* **Shareware**: Shareware is licensed software that the organization has purchased for a specific period. Ensure the license is up to date or discontinue use if it is expired.
* **Reputable Sources**: Verify that the shareware is from a reputable source and free of malware.
* **Approval Process**: Obtain approval from the cybersecurity team and legal department before implementing any shareware to ensure compliance and security.

**Software Piracy Rules and Consequences**

* **Compliance**: All employees must adhere to software piracy rules to ensure compliance.
* **Usage**: Use licensed software only for its intended purpose.
* **Audits**: Regular audits will be conducted to ensure all software is up to date and used appropriately.
* **Reporting**: Report any illegal software usage to the Business Software Alliance (BSA).

By following these guidelines, we ensure a secure and legally compliant work environment. If you have any questions or need further clarification, please reach out to the IT or legal department.

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

### **Ajax Corporation Code of Conduct: Privacy in the Workplace**

At Ajax Corporation, we are committed to ensuring that our employees understand their rights and the workplace privacy laws that we adhere to. Below are the key guidelines regarding workplace monitoring and privacy:

#### **Workplace Monitoring**

**Monitoring**: All assets belonging to Ajax Corporation are subject to monitoring. This includes emails, internet logs, chats, and phone conversations (both calls and texts). Personal belongings will remain private unless they are left at the workplace or are part of an investigation into a reported crime. Monitoring is conducted to ensure compliance with company policies, protect company assets, and maintain a secure work environment.

**Health Records**: We advise employees to keep their personal health records off-site. These records are personal and will not be subject to search by the company. This is in compliance with the Health Insurance Portability and Accountability Act (HIPAA), which mandates the confidentiality of health information.

**Surveillance**: Due to the sensitive nature of the information technology within our organization, employees are monitored under 24/7 surveillance. Surveillance is limited to common areas and does not extend to private spaces such as restrooms or locker rooms. This practice is in line with industry standards to ensure the safety and security of both employees and company assets.

Your privacy is of utmost importance to us, and we take it very seriously.

#### **Secure Communications**

**General Data Protection Regulation (GDPR)**: We comply with current GDPR guidelines for data collection and protection. This includes ensuring that personal data is processed lawfully, fairly, and transparently. Employees have the right to access their personal data and request corrections if necessary.

**Data Surveillance**: We adhere to established guidelines for data surveillance to ensure the protection of employee privacy. Data collected through surveillance is used solely for legitimate business purposes and is stored securely to prevent unauthorized access.

#### **Protecting Privacy**

We are dedicated to protecting the privacy of our employees and ensuring that all monitoring practices are conducted ethically and transparently. Employees are informed about monitoring practices through the employee handbook and regular training sessions. We also conduct periodic reviews of our monitoring practices to ensure they remain compliant with legal standards and industry best practices.

#### **Consequences of Policy Violations**

Violations of these established policies will result in appropriate disciplinary actions, up to and including termination of employment. Disciplinary actions are determined based on the severity of the violation and are conducted in a fair and consistent manner.

#### **Appeal Process**

Employees have the right to appeal any disciplinary actions taken against them. The appeal process is outlined in the employee handbook and includes steps for submitting an appeal, the review process, and timelines for resolution. Employees are encouraged to provide any supporting documentation or evidence as part of their appeal.

#### **Contact Information**

For any questions or concerns regarding these policies, please contact the Human Resources department. The HR department is available to provide guidance and support on privacy-related matters and can be reached via email or phone.

#### **Disclosure**

There will be no discrimination against employees who report ethical violations. Employees can report these violations anonymously through the designated reporting channels. We have a zero-tolerance policy for retaliation against employees who raise concerns in good faith.

By adhering to these guidelines, we aim to create a secure and respectful workplace for all employees. If you have any questions or need further clarification, please do not hesitate to reach out.

**References**

*Code of Conduct & Ethics (Examples and Best Practices)*. (2023, May 5). Status.net. <https://status.net/articles/code-of-conduct-and-ethics-what-to-include-with-examples/>

Reynolds, G. (2018). *Ethics in information technology*. Cengage Learning.

*8 Top Strategies for Cybersecurity Risk Mitigation - SecurityScorecard*. (2024, July 1). SecurityScorecard. <https://securityscorecard.com/blog/8-top-strategies-for-cybersecurity-risk-mitigation/>

Institute of Data. (2023, November 12). The Essential Software Engineering Code of Ethics | Institute of Data. *Institute of Data*. <https://www.institutedata.com/us/blog/software-engineering-code-of-ethics/>

LRN. (n.d.). *Privacy Policy | LRN Corporation*. <https://lrn.com/privacy-policy>

Neagu, C. (2024, January 25). *How to conduct a cybersecurity risk assessment (2024)*. Heimdal Security Blog. <https://heimdalsecurity.com/blog/cybersecurity-risk-assessment/>