A1/A1a. Ethical Guidelines Related to Information Security

An ethical guideline that should have been implemented in TechFite is the Integrity and Confidentiality Principle from the IAPP Code of Ethics. This guideline requires an organization to maintain the highest levels of data integrity by preventing unauthorized access or disclosure of proprietary and confidential data. In the case study, Tech Fite's Application Division, led by Carl Jaspers, violated this ethical standard when proprietary information owned by Orange Leaf Software and Union City Electronic Ventures was used in a way that competitors launched similar products. If TechFite had followed this ethical standard, policies would have been in place to segregate client data and ensure that confidential information was not open to unauthorized access or exploitation (International Association of Privacy Professionals, 2020).

Another relevant ethical guideline is the Principle of Least Privilege (PoLP) from the (ISC)2 Code of Ethics. PoLP states that employees should be granted only minimal access to perform their job functions to avoid any risk of illegitimate data access or manipulation. However, at TechFite, every workstation and computer had full administrative rights, including the Business Intelligence and marketing/sales units. Employees like Sarah Miller, Megan Rogers, and Jack Hudson had unrestricted visibility across units, which enabled unapproved and manipulation of sensitive client information. This ethical standard would have prevented unauthorized access to confidential data by restricting permissions and enforcing accountability, thus reducing unethical behavior (ISC^2, 2022)

A2. Unethical Practices

One of the most apparent unethical practices in the TechFite case was the unauthorized access and misuse of client proprietary data. The head of the Applications Division, Carl Jaspers, gathered sensitive business intelligence from potential clients through consultation questionnaires, even though those companies later declined TechFite's services. Both Orange Leaf Software, represented by CEO Noah Stevenson, and Union City Electronic Ventures, represented by CTO Ana Capperson, fell victim to this practice. Their proprietary information was later found in the hands of competitors who were already TechFite clients. This unethical behavior violated trust and confidentiality because client data was used for competitive advantage instead of being stored and protected as proprietary information.

Another unethical practice was the creation and continued use of dummy accounts in TechFite. These accounts, which Carl Jaspers requested, belonged to former employees but were still active and were used for intelligence-gathering purposes, including disallowed penetration testing and surveillance of computer networks. Emails linked to

these accounts referenced unethical intelligence-gathering methods such as dumpster diving and trash surveillance. These emails were sent to parties outside TechFite, indicating a widespread misapply of company resources for covert operations. This action was unethical and potentially illegal because it involved unauthorized access to information systems. Exploitation of these accounts reveals serious ethical failings in access control and accountability in the organization.

A3. Factors

Lack of internal oversight and auditing was a major contributing factor to TechFite's lax ethical behavior. The BI Unit did not have adequate documentation on internal security practices and no formal processes for auditing user accounts, privilege escalations, or data segregation. For example, IT security Analyst Nadia Johnson, who was responsible for reviewing reports for CISOE, never audited the client list database. Employees had unchecked access to sensitive information, allowing for data misuse and disallowed access to competitor information. With a robust auditing framework in place, many of these unethical behaviors could have been caught and stopped early.

Conflicts of interest and favoritism within TechFite's organizational culture were another factor. The case study revealed that IT security analyst Nadia Johnson consistently got positive recommendations and raises from Carl Jaspers despite not performing necessary internal audits. In addition, her social media activity suggested a close personal relationship with Jaspers, including attending social events hosted by him and receiving birthday gifts from him, raising questions about impartiality in IT security oversight. This separation between security personnel and leadership allowed for unethical behaviors to flourish without consequence.

B1. Information Security Policies

A Data Loss Prevention (DLP) Policy is one security policy that could have prevented unethical practices at TechFite. A robust DLP policy would protect proprietary client information and would flag and investigate any attempt to transfer or share sensitive data outside authorized channels. For example, if DLP measures had been in place, the unwarranted flow of proprietary information from Orange Leaf Software and Union City Electronic Ventures to their competitors would have been detected and blocked. This policy could have prevented intellectual property theft and protected client trust.

Another security policy that should have been implemented is the User Account Management Policy. This policy would develop guidelines for creating, controlling, and deleting user accounts, with the aim of getting accounts of former employees eliminated or disabled. This policy could have prevented the misuse of the ghost accounts created by

Carl Jaspers for intelligence-gathering purposes. In addition, privileged escalation monitoring and role-based access controls may have curtailed unauthorized access to sensitive organizational data.

B2. SATE Components

A Mandatory Annual Security Training under the direct oversight of an independent compliance officer is a key component that should be implemented in TechFite's SATE program. This training would educate employees on ethical information security practices, legal obligations, and company data handling and confidentiality policies. Providing all employees with annual training can help TechFite build a culture of compliance and reduce the risk of ethical and legal violations.

A second component of the SATE program should be Strict Enforcement of Non-Compliance Repercussions. Employees who violate security policies (unauthorized access to client data or misuse of privileged accounts) should be fired (terminated or legalized). A stipulation of punishment for unethical behavior would deter employees from engaging in improper conduct and foster an ethical cybersecurity culture.

B2a. SATE Program Communication

Communication of the SATE program to employees should be done through multiple channels. An initial announcement regarding the purpose, scope, and requirements of the program must be made via an official CISO email. This should be followed by an all-hands meeting where employees are given direct instructions on training schedules and compliance expectations. There should also be an internal portal for employees to access training materials, policy documents, and reporting mechanisms for ethical concerns.

B2b. SATE Program Justification

One of the unacceptable behaviors we discussed earlier was the misuse of proprietary client information. To counter this, a training module of the SATE program should cover data privacy and the legal and ethical implications of data mismanagement. Employees should be educated on confidentiality agreements and the consequences of breaching client trust.

Another unethical behavior was the use of ghost user accounts for intelligence-gathering purposes. To address this issue, the SATE program should include training on access controls and user account management. Employees must understand the importance of unauthorized access. Training on ethical hacking principles should also be provided to prevent the abuse of penetration testing tools within the organization.

C. Ethics Issues and Mitigation Summary for Management

TechFite's Application division has abused proprietary client information, gained prohibited access to competitor networks, and mishandled user accounts. This has resulted in unethical business practices, including unallowed penetration testing, social engineering, and misrepresenting sales figures through fake clients like Bebop Software, FGH Research Group, and Dazzling Comet Software. All these actions have led to vast breaches of trust and confidentiality, a terrible reputation for the company, and likely will lead to legal troubles. Lack of internal oversight, conflicts of interest, and absence of formal security policies have created an unethical organizational culture.

To prevent them, TechFite needs strong security policies, such as a Data Loss Prevention Policy and a User Account Management Policy, to manage data and control access. It should also introduce a SATE program to educate employees on ethical cybersecurity practices and impose fines on those who do not comply. TechFite can avert future ethical violations and prevent further harm to its stakeholders by creating a culture of accountability and enforcing security measures.

Reference:

International Association of Privacy Professionals (IAPP). (2020). *Privacy and data protection ethics*. https://iapp.org

(ISC)^2. (2022). *(ISC)^2 Code of Ethics*. International Information System Security Certification Consortium. https://www.isc2.org/Ethics