**A. Address ethical issues for cybersecurity by doing the following:**

1. **Discuss the ethical guidelines or standards relating to information security that should apply to the case study.** Adherence to the NDA, respect for privacy, compliance and oversight and data protection and privacy. One ethical guideline that should apply to this case is responsible disclosure, another one would be professional competence.

a. **Justify your reasoning.** NDA also known as non disclosure agreement has a legal component, ethical component and a reputation component. If a NDA is broken, legal action can be taken, companies also have an ethical component because there was an agreement and we should always have integrity and high morals. If we break an NDA our reputation is also on the line because other organizations will not want to do business with us. Respect for privacy gains trust in customers and breaking this can lead to legal consequences and loss of customers. Compliance and oversight means that everyone in the company is being held accountable for their actions, the BI unit has had a lack of safeguarding information and accountability. Data protection and privacy is needed because the data of the clients got leaked. They would do this by implementing Data loss prevention methods and not disclosing the data of their clients. Responsible disclosure means that when a vulnerability is found the victim is contacted immediately rather than having their systems be penetration tested. The applications division within the company should definitely have handled things differently. Professional competence means that people hired have the necessary skills to perform their job and not bottleneck the company with their lack of skills. Nadia Johnson received unfair treatment, was given raises and different treatment than others, she was incompetent because she did not audit IT user accounts and breaches.

**2. Identify the behaviors, or omission of behaviors, of the people who fostered the unethical practices.** Carl Jaspers who was the head of the applications division failed to respect the NDA with clients and allowqed unauthorized access to customer data, there was a lack to separate client data in the BI Unit, which lead to lax oversight over user data. Jasper’s also had a bias for Nadia Johnson. There was no policy that prohibited social relationships between the company and this led to biases which gave Nadia raises and special treatment. The Bi unit also used fake accounts to gain access to data within the company without authorization. There was no effort to enforce the separation of duties principle of least privilege principle.

3.  **Discuss what factors at TechFite led to lax ethical behavior.** One factor that led to lax behavior was lack of accountability, one example of this is when the NDA was breached and no one was punished. If there is no accountability employees will not follow rules. Another was lack of policies. One example of this was they did not have a policy for social relationships in the company which led to the favoritism mentioned before, another example was a lack of training on ethics and security. Without this employees do not understand the consequences of what they do.

B. **Describe ways to mitigate problems and build security awareness by doing the following:**

1. Describe **two** information security policies that may have prevented or reduced the criminal activity, deterred the negligent acts, and decreased the threats to intellectual property. One of the information security policies that could be implemented would be an employee termination policy, this means that after an employee does an act that is unacceptable they will have an exit interview and the company’s devices will be given back to the company. Another is intellectual property protection policy, this means that intellectual property needs to be defined and audits will be done to make sure that it is safe, apart from this there needs to be training and awareness in the employees of this issue.

2.  **Describe the key components of a Security Awareness Training and Education (SATE) program that could be implemented at TechFite.** They key components of a SATE program include: training in phishing, passwords, new threats, physical and device security,support from management, and incident response.

a. **Explain how the SATE program will be communicated to TechFite employees.**An initial email will be sent to all employees along with follow up emails about new threats. A custom security course will be mandatory for employees to take. An initial meeting will be held in person along with follow up meetings every determined amount of time in between.

b. **Justify the SATE program’s relevance to mitigating the undesirable behaviors at TechFite.** There are many reasons why a SATE program would be beneficial. ONe such reason is that insider threats would be reduced substantially. Another reason is it would create a security conscious culture which means that employees are always thinking of security and may even be stopped from stealing information from the company. Another is meeting compliance requirements from industry specific requirements. This stops unwanted outcomes and legal consequences of not following the requirements.

C. **Prepare a summary directed to senior management (*suggested length of 1–2 paragraphs*) that states TechFite’s ethical issues from Part A and the related mitigation strategies from Part B.**

Part A of our examination focused on the serious moral problems that TechFite faces. Concerning practices have been shown, especially by the Applications Division. These include potential violations of non-disclosure agreements, insufficient safeguarding of customer information, and illegal data access and favoritism and bias to employees . This type of conduct puts the business at risk for legal and regulatory issues in addition to harming its brand and reputation.

We suggest a detailed and thorough Security Awareness Training and Education (SATE) program, described in Part B, to address these ethical concerns. The goal of this program is to establish a culture of security awareness by highlighting the significance of non-disclosure agreements, data handling protocols, and access controls. Through the creation of a security-aware atmosphere and the establishment of strong regulations, we may reduce unwanted behaviors within the company, encourage moral information practices, and improve overall information assurance and security. TechFite is protected against any problems at any angle by this strategic strategy, which also complies with legal requirements and industry best practices.