1. When policies are unclear, individuals must rely on their own ethical judgment to make decisions. Varying ethical judgments can be influenced by personal values, cultural background, and the situation at hand. The absence of clear policies can result in decisions that do not align with an organization's values and goals. However, unclear policies also allow individuals to exercise creativity appropriate for the scenario. This might be beneficial and increase productivity under certain circumstances.

To maintain consistency and uphold ethical values, organizations must provide clear policies that outline expectations and standards of behavior. Policies serve as a standard to hold employees accountable for their actions. Ethics training and guidance from leaders and colleagues are necessary to foster a culture of ethical behavior within the organization.

A culture of ethical behavior promotes transparency, honesty, and integrity in decision-making, where employees prioritize the organization's values and mission over their self-interests. In situations where policies are not clear or do not address a specific ethical dilemma, individuals must rely on their own ethical judgment and seek guidance from others.

2. Safeguarding customers' information is essential for organizations, particularly for financial institutions that deal with sensitive financial data. A policy ensuring no unauthorized access to customers' information is vital in protecting the bank's reputation and customer trust. To achieve this, the policy should contain guidelines for access control, user authentication, and data encryption. Only employees who require access to perform their job functions should be permitted access to customer data. User authentication should utilize strong passwords and multi-factor authentication, while data encryption should protect sensitive data both at rest and in transit. Compliance monitoring and regular audits are essential to ensure policy adherence.

However, relying on policies and guidelines may not be sufficient to secure sensitive customer data. The zero-trust security model assumes that nobody can be trusted until verified, emphasizing network and micro-segmentation, identity and access management solutions, and other advanced technologies for safeguarding sensitive data.

Implementing a culture of security awareness and training is critical to ensuring customer data security. Educating employees on the significance of protecting customer information and the consequence of unauthorized access is essential to creating a security-aware culture that improves the overall security posture of the bank.

Finally, the team should conduct regular penetration testing and vulnerability assessments to identify and address system security weaknesses. This proactive approach prevents potential data breaches and ensures customer data protection.

3. Although Troy University's anti-cheating system is designed to prevent cheating on tests and assignments, it raises ethical concerns.

Using such systems to monitor employees can violate privacy and trust, suggesting that employers do not trust their employees to act ethically without constant surveillance. It can create suspicion and distrust within the workplace, leading to false positives and innocent employees being punished for perceived ethical violations. If the monitored behavior is directly related to job responsibilities and done transparently and fairly, it may be seen as necessary to ensure ethical standards are upheld. For example, if an employee's job involves handling sensitive information, monitoring their computer activity may be necessary to ensure confidential information is not accessed or shared.

It is crucial to balance promoting ethical behavior and respecting employees' privacy and trust. Employers have a responsibility to maintain an ethical workplace adhering to fair play and honesty. However, monitoring employees could invade privacy, erode trust, and compromise autonomy and independence, leading to resentment and demotivation.

Ultimately, using monitoring technology in the workplace must consider potential benefits and risks. Employers must ensure implementation respects privacy and autonomy, used for legitimate purposes rather than surveillance or control. Employees must be informed and given the opportunity to provide feedback.