PassQueen
a.k.a dumpsqueen.com

WGU Ethics In TechnologyQCO1

WGU Ethics-In-Technology

Version Demo

Total Demo Questions: 8

Total Premium Questions: 81

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An incident handler discovers an unauthorized change in the security key vault's database file, which caused a disclosure of confidential information. Which ethical issue does this incident pose?

A. Property

B. Privacy

C. Access

D. Accuracy

ANSWER: B

Explanation:

Privacy is the ethical issue posed because the unauthorized alteration resulted in confidential information being disclosed to parties who were not authorized to receive it. In technology ethics, privacy concerns an individual's or organization's ability to control sensitive information and to expect that such information will be collected, used, stored, and disclosed only under appropriate authority. A security key vault is specifically intended to protect highly sensitive cryptographic material and related confidential data. When its database is altered in a manner that exposes protected information, the core ethical harm is the loss of confidentiality and the resulting invasion of privacy interests. Responsible technology practice requires incident handlers and organizations to safeguard sensitive information throughout its lifecycle, limit access to authorized users, and promptly contain and remediate disclosures. This expectation is reflected in the ACM Code of Ethics, which directs computing professionals to respect privacy and maintain the confidentiality of information. It also aligns with the NIST Cybersecurity Framework's protection objective of using safeguards to ensure delivery of critical services and limit the impact of cybersecurity events. See the ACM Code of Ethics and Professional Conduct and the NIST Cybersecurity Framework.

QUESTION NO: 2

To gather data for improved customer profiles, a social media platform uses microphone data from its users in the United States. Which U.S. Constitulional amendment does this action violate?

A. Third Amendment

B. Fourth Amendment

C. Second Amendment

D. First Amendment

E. None of these—the conduct described does not itself violate a U.S. Constitutional amendment.

ANSWER: E

Explanation:

"None of these—the conduct described does not itself violate a U.S. Constitutional amendment" is correct because constitutional protections, including the Fourth Amendment's protection against unreasonable searches and seizures, generally restrict government action rather than the actions of a private social media company. The question identifies a platform collecting microphone data for customer profiling but does not state that a government agency directed, compelled, jointly participated in, or otherwise transformed the company's conduct into state action. Without that essential government connection, the conduct cannot, by itself, be characterized as a violation of the Fourth Amendment or another constitutional amendment.

That conclusion does not mean the collection is necessarily permissible. Depending on the facts, such collection may create significant privacy, consent, consumer-protection, wiretapping, contract, or state-law concerns. For example, laws and platform disclosures may require meaningful notice and consent for microphone access or for the use of information

collected through an application. Those are statutory, regulatory, and ethical issues, however, rather than an automatic constitutional violation. The Supreme Court has consistently recognized the state-action requirement for constitutional claims involving private entities. See the Fourth Amendment text and interpretation from Cornell Law School and Manhattan Community Access Corp. v. Halleck, addressing the general rule that constitutional rights protect against governmental, not private, conduct.

QUESTION NO: 3

A university uses a cloud service to host course materials, assignments, and student grades. The service provider requests permission to use identifiable student records to develop unrelated commercial analytics products.

Which two actions best support the university's responsibility to protect student education records? Choose 2 answers.

A. Permit the provider to use identifiable records for unrelated commercial analytics

B. Limit the provider's access and use to the contracted educational service

C. Establish written controls for access, security, retention, and deletion

D. Publish the records so all students can verify the data

E. Require the provider to retain all records indefinitely

ANSWER: B C

Explanation:

The university should **limit the provider's access and use of student records to the contracted educational service** and **establish written controls for access, security, retention, and deletion of the records**. Student grades and assignments are education records, and a provider acting for the institution should handle them only for authorized institutional purposes with appropriate safeguards.

Using identifiable records for the provider's unrelated commercial analytics purpose exceeds the educational-service purpose described in the scenario. Publicly posting records would create a serious privacy issue. Indefinite retention is inconsistent with responsible data-governance practices because records should not be kept longer than necessary for a valid purpose.

QUESTION NO: 4

An organization is concerned about its cybersecurity after identifying unauthorized records in its payroll database. The organization hires a consultant to test its cyberdefenses. The consultant executes several test attacks on the organization's software and successfully demonstrates that by using Structured Query Language (SOL) injection, the consultant can add rows to the payroll database without obtaining the proper permissions.

Which hacker classification does the consultant fall under?

A. Cybercriminal

B. White hat hacker

C. Cyberterrorist

D. Black hat hacker

ANSWER: B

Explanation:

White hat hacker is correct because the consultant was explicitly hired by the organization to assess the security of its systems. White hat hackers, also called ethical hackers, use attacker-like techniques in an authorized engagement to identify, validate, and report security weaknesses so the organization can remediate them. Here, demonstrating that an

injection vulnerability permits unauthorized additions to payroll records establishes a meaningful security finding: the application appears to accept untrusted input in a way that can alter database data without appropriate authorization controls.

The consultant's authorization and defensive purpose are the key facts. An ethical security test is performed within an agreed scope, such as identified applications, systems, and testing methods, and the resulting evidence is provided to the system owner for risk reduction. The finding can help the organization implement parameterized queries, input validation, least-privilege database accounts, and appropriate authorization checks. The National Institute of Standards and Technology describes penetration testing as a process for identifying vulnerabilities through simulated attacks, while OWASP provides guidance on preventing injection flaws in web applications. See NIST SP 800-115: Technical Guide to Information Security Testing and Assessment and OWASP Top 10: Injection.

QUESTION NO: 5

A payroll application has experienced several incidents in which employee bank-account information was altered after a supervisor's account was compromised. The organization wants to strengthen the integrity of payroll records.

Which two controls most directly address this risk? Choose 2 answers.

A. Require independent approval for changes to bank-account information

B. Maintain and review audit logs of payroll-record modifications

C. Encrypt all payroll records without changing authorization procedures

D. Increase database storage capacity for payroll information

E. Send employees a general newsletter about cybersecurity

ANSWER: A B

Explanation:

Requiring independent approval for changes to bank-account information reduces the chance that one compromised account can make an unauthorized change without review. Maintaining audit logs and regularly reviewing them creates accountability and helps detect unexpected modifications to sensitive payroll records.

Encrypting records protects confidentiality but does not by itself prevent an authorized or compromised account from changing information. Increasing storage capacity addresses availability rather than accuracy and authorized modification. Sending a general security newsletter may be useful awareness activity, but it is less direct than controls over the high-risk change process.

QUESTION NO: 6

A transportation application collects trip histories to calculate fares and provide customer support. The company is revising its privacy program using the Organisation for Economic Co-operation and Development (OECD) privacy guidelines.

Which two practices are most consistent with the purpose specification and use limitation principles? Choose 2 answers.

A. State the purposes for collecting trip histories when the information is collected

B. Limit later use to specified or compatible purposes with appropriate authority

C. Use trip histories for any profitable purpose after collection

D. Keep data-collection purposes confidential from customers

E. Provide unrestricted internal access to all trip histories

ANSWER: A B

Explanation:

The company should specify the purposes for collecting trip histories no later than when the data is collected and limit later use to those purposes or to compatible purposes supported by appropriate authority. These practices make collection and subsequent use more transparent and reduce the risk that information will be repurposed in ways customers would not reasonably expect.

Using trip histories for any profitable purpose is inconsistent with use limitation. Keeping purposes confidential from customers conflicts with purpose specification. Providing unlimited internal access to trip histories does not limit use and creates additional privacy and confidentiality risks.

QUESTION NO: 7

A health technology company is preparing to deploy an artificial intelligence system that recommends follow-up care after hospital discharge. Historical data show that some rural communities have less complete follow-up documentation than urban communities.

Which two actions should the company take before deployment to reduce the risk of unfair recommendations? Choose 2 answers.

A. Evaluate recommendation outcomes across relevant communities

B. Review the data for incomplete or unrepresentative follow-up records

C. Remove every geographic field without evaluating its purpose or effects

D. Deploy the system and wait for patients to report unfair outcomes

E. Increase the total number of records without examining subgroup coverage

ANSWER: A B

Explanation:

The company should evaluate performance across relevant communities and investigate the completeness and representativeness of the historical data. Missing or uneven documentation can cause a model to learn patterns that reflect access differences rather than patients' actual care needs. Testing outcomes by relevant groups can reveal whether similarly situated patients receive materially different recommendations.

Removing all geographic information without analysis is not necessarily an effective mitigation because location may be relevant to available services and can also be represented by other variables. Deploying first and addressing complaints later fails to manage a known risk. Increasing the overall data volume also does not resolve systematic underrepresentation or incomplete records for a particular community.

QUESTION NO: 8

A company has used Its credit approval system for a long time. A risk evaluation director initiates an update of the data model to make sure it meets the highest ethical standards. Which Software Engineering Code of Ethics and Professional Practice principle does the director's action represent?

A. Management

B. Colleagues

C. Self

D. Judgment

ANSWER: D

Explanation:

Judgment is correct because the director is exercising professional judgment to ensure that a consequential technical artifact—the credit-approval data model—continues to meet ethical expectations. Credit decisions can materially affect people's access to housing, employment, education, and financial opportunity. Reviewing and updating a long-used model is therefore not merely a maintenance task; it requires an independent, ethically grounded assessment of whether the model's assumptions, data use, outcomes, and potential biases remain appropriate. The Software Engineering Code of Ethics states that software engineers should maintain integrity and independence in their professional judgment. It also directs practitioners to temper technical judgments with the need to support and maintain human values. By proactively initiating a review aimed at the highest ethical standards, the director applies those responsibilities to a system whose outputs may have significant effects on individuals. This principle supports evaluating whether the model remains fair, trustworthy, and aligned with human values as data, business practices, and social expectations change. The full code is available from the ACM Software Engineering Code of Ethics and Professional Practice; its professional-judgment provisions are also reproduced by the ACM Ethics site.