Question 1 **[Security Principles]** Rob accidentally downloaded a malware that leverages ambient authority. That malware uploaded all Rob's files (both on their laptop and accessible as shared folders) to a cloud. The company discovers later that during the same leak, documents in other departments, that Rob was not working on, also got leaked due to the malware. Which security principle(s) were incorrectly applied by the company's system administrators that manage the shared folders and allowed the full leak ?

- ☐ Fail-Safe Default
- ☒ Least Privilege
- ☐ Psychological Acceptability
- ☐ Separation of Privilege

Question 2 **[Access Control]** Which of the following are true about Access Control Lists?

- ☐ They associate permissions to subjects.
- ☐ It is easy and efficient to determine a given user's permissions on all files.
- ☒ They associate permissions to objects.
- ☒ It is easy and efficient to revoke rights by resource.

Question 3 **[Access Control]** MAC stands for Mandatory Access control in this question with levels secret $<$ top secret. Which of the following statements are true?

- ☐ A system designed using MAC automatically follows the least privilege principle.
- ☐ MAC and DAC cannot coexist within the same system.
- ☒ BLP does not guarantee that top secret information cannot be accessed by the lowest clearance subjects.
- ☐ In MAC, owners can delegate access to a document to any user.

Question 4 **[Symmetric Cryptography]** In symmetric cryptography, there are two types of ciphers: stream ciphers and block ciphers. Block ciphers have different modes of operation. Which of the following statements are true?

- ☒ When using a block cipher in ECB mode, the encryption of a block does not include information from any other block.
- ☐ CTR mode is not secure if the nonce is reused under two different keys.
- ☐ When using a stream cipher, both the key and the initialization vector (IV) must be kept secret.
- ☒ CBC mode is not secure if the IV is reused under the same key.

Question 5 **[Cryptography]** Which of the following statements are true?

- ☒ **Encrypt(key, m) = c**, where **c** is a random string, is not a valid form of encryption that provides confidentiality.
- ☐ All encryption schemes guarantee that the risk that an adversary without the secret key can read the plaintext is 0.
- ☐ Applying twice a hash function, i.e., **hash(hash(m))** is less secure than applying it only once.
- ☐ In digital signatures, the secret key is used to verify the signature given a message.

Question 6 **[Authentication]** Which of the following statements are true?

- ☐ Authentication is a process that determines whether a subject has permission to use a resource or access a file.
- ☐ Encrypting the channel prevents replay attacks during a network-based authentication process.
- ☒ Storing a salted hash instead of a password does not prevent brute-force attacks.
- ☐ In biometrics-based systems, a low rate of false positives is always more important than a low rate of false negatives.