Question 1

A system administrator has created the following "array" as an access control for an organisation.

Developers: create files, update files.

Reviewers: upload files, update files.

Administrators: upload files, delete fifes, update files.

What type of access-control has just been created?

Options:

A- Task based access control.

B- Role based access control.

C- Rule based access control.

D- Mandatory access control.

Answer:

C

Question 2

As well as being permitted to access, create, modify and delete information, what right does an Information Owner NORMALLY have in regard to their information?

Options:

A- To assign access privileges to others.

B- To modify associated information that may lead to inappropriate disclosure.

C- To access information held in the same format and file structure.

D- To delete all indexed data in the dataset.

Answer:

B

Question 3

What term is used to describe the act of checking out a privileged account password in a manner that bypasses normal access controls procedures during a critical emergency situation?

Options:

A- Privileged User Gateway

B- Enterprise Security Management

C- Multi Factor Authentication.

D- Break Glass

Answer:

C

Question 4

Question Type: **MultipleChoice**

What are the different methods that can be used as access controls?

1. Detective.

2. Physical.

3. Reactive.

4. Virtual.

5. Preventive.

Options:

A- 1, 2 and 4.

B- 1, 2 and 3.

C- 1, 2 and 5.

D- 3, 4 and 5.

Answer:

C

Question 5

What aspect of an employee's contract of employment Is designed to prevent the unauthorised release of confidential data to third parties even after an employee has left their employment?

Options:

A- Segregation of Duties.

B- Non-disclosure.

C- Acceptable use policy.

D- Security clearance.

Answer:

B

Question 6

Question Type: **MultipleChoice**

What term refers to the shared set of values within an organisation that determine how people are expected to behave in regard to information security?

Options:

A- Code of Ethics.

B- Security Culture.

C- System Operating Procedures.

D- Security Policy Framework.

https://www.cpni.gov.uk/developing-security-culture#:~:text=Developing%20a%20Security%20Culture,-What%20type%20of&text=Security%20culture%20refers%20to%20the,think%20about%20and%20approach%20security.&text=Employees%20are%

Answer:

B

Question 7

Question Type: **MultipleChoice**

Select the document that is MOST LIKELY to contain direction covering the security and utilisation of all an organisation's information and IT equipment, as well as email, internet and telephony.

Options:

A- Cryptographic Statement.

B- Security Policy Framework.

C- Acceptable Usage Policy.

D- Business Continuity Plan.

Answer:

A

Question 8

Question Type: MultipleChoice

When considering outsourcing the processing of data, which two legal "duty of care" considerations SHOULD the original data owner make?

1 Third party is competent to process the data securely.

2. Observes the same high standards as data owner.

3. Processes the data wherever the data can be transferred.

4. Archive the data for long term third party's own usage.

Options:

A- 2 and 3.

B- 3 and 4.

C- 1 and 4.

D- 1 and 2.

Answer:

C

Question 9

Question Type: **MultipleChoice**

What form of attack against an employee has the MOST impact on their compliance with the organisation's "code of conduct"?

Options:

A- Brute Force Attack.

B- Social Engineering.

C- Ransomware.

D- Denial of Service.

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which term is used to describe the set of processes that analyses code to ensure defined coding practices are being followed?

Options:

A- Quality Assurance and Control

B- Dynamic verification.

C- Static verification.

D- Source code analysis.

Answer:

D