SYLLABUS & WEIGHTAGE FOR
COMPUTER BASED TEST
ADVERTISEMENT No: 12/2026/CHQ/DR-CBT

MANAGER (INFORMATION TECHNOLOGY)

Total Marks: 120 **Duration: Two hours**

Part-A

General Knowledge, General Intelligence, General Aptitude, English etc. — Weightage 50%

Part-B

Questions on subjects relating to Educational Qualifications — Weightage 50%

1. Programming Languages:

(i) Proficient in Python, R, and SQL, facilitating advanced data analysis, statistical computing, and efficient database management. Experienced with AI and machine learning libraries such as TensorFlow, PyTorch, scikit-learn, and Keras for developing and deploying intelligent models.

(ii) **ABAP** for SAP ERP backend development and customization.

SAPUI5 / Fiori (JavaScript) essential for front-end development.

- Skilled with **SQL** and **Java** language for SAP interface development especially for integrations and advanced customizations.
- SAP HANA SQL Script:

  Extended SQL scripting language used for SAP HANA database procedures.
- OData Protocol:

  For enabling data services and APIs in SAP.
- BAPIs & IDocs:
- SAP-**specific interfaces often accessed via ABAP.**

2. Data Augmentation Technologies:

Experience with big data tools and frameworks such as Hadoop and Apache Spark, as well as MXNet —a scalable deep learning framework supported by Apache that offers efficient training and deployment with robust multi-language support. These technologies are used to process and analyze large-scale datasets, enhancing and managing complex data to improve quality, diversity, and usability for analytics and machine learning. They enable handling data at scale, facilitating efficient data augmentation through both batch and real-time processing.

(i) Data Transformation & Enrichment:

Tools and processes that clean, normalize, and enrich raw data by adding new information or creating synthetic data to improve model training and accuracy.

(ii) Automated Data Generation:

Techniques that create new **training data from** existing datasets using methods like image rotation, cropping, noise addition (especially in AI/ML), enhancing model robustness.

(iii) Integration with Cloud Services:

Skilled in **leveraging cloud computing services** including AWS, Azure, and Google Cloud for scalable infrastructure, data storage, and deployment. Leveraging cloud-based data augmentation **pipelines** to scale operations, ensure high availability, and facilitate seamless data flow across platforms.

3. API Programming:

Expertise in designing, developing, and consuming APIs using protocols like REST, SOAP, and GraphQL etc.

(i) Proficient in API framework development to facilitate seamless data exchange and functionality sharing between different software systems.

(ii) Enables modular development where one team can build APIs while others integrate them without needing to know the internal implementation.

(iii) Powers microservices architecture and modern cloud-native applications, fostering flexibility and scalability.

(iv) Supports integration across diverse platforms including mobile, web, and desktop environments.

4. Cybersecurity Fundamentals:

Basic knowledge of key security domains and core security concepts, including **threat vectors, types of cyberattacks,** and common **vulnerabilities.**

(i) **Network Security:** Protects data as it travels across networks like Wi-Fi, LAN, VLAN, corporate LANs, and cloud environments. It aims to prevent unauthorized access, data breaches, and disruptions by ensuring data confidentiality, integrity, and availability during transmission.

Key Components:

Firewalls: Regulate network traffic based on security policies.

VPNs: Encrypt data for secure communication over public networks.

IDS/IPS: Detect and block suspicious network activity.

Encryption: Secures data during transmission (e.g., HTTPS, TLS).

Network Segmentation: Limits access by dividing networks to contain threats.

Endpoint security: Safeguarding user devices.

Cloud security: Ensuring security in cloud environments.

(ii) Common Elements in Data Protection Frameworks

Data Classification: Organizing data based on its level of sensitivity, and it's application of appropriate protection measures.

Access Controls: Role-based access management of data, and prevent unauthorized use.

Encryption: Securing data both while stored (at rest), and during transmission to protect confidentiality.

Data Minimization: Limiting data collection or windowing of data management.

Windowing: Method of dividing continuous or large datasets into smaller, manageable chunks called "windows" for processing or analysis over specific time intervals or data counts. This approach enables efficient, real-time data analysis by focusing on relevant subsets instead of the entire dataset.

Types of Windows

Tumbling Window: Fixed, non-overlapping intervals.

Sliding Window: Overlapping intervals that move forward incrementally.

Session Window: Defined by periods of activity separated by inactivity.

Count-based Window: Based on a fixed number of data points.

Audit and Monitoring: Continuously tracking and reviewing data access and usage to detect anomalies or misuse.

Incident Response: Establishing clear procedures to quickly address and mitigate data breaches or leaks.

Data Subject Rights: Ensuring individuals can access, correct, or delete their personal data as required by law.

Data protection practices and policies.

(iii) Cybersecurity dashboarding

This is real-time, visual interfaces that consolidate critical security metrics, alerts, and trends to enable security teams to monitor, analyze, and respond to threats efficiently.

Centralize security posture visibility

Rapidly identify and prioritize incidents

Monitor compliance and risk metrics

Facilitate informed decision-making with actionable insights

Visualizations like charts, heat maps, and timelines.

Real-time alerts and notifications.

Incident tracking and summaries.

Vulnerability and patch status.

User activity and access logs.

*****