बरिष्ठ प्रबन्धक (सूचना प्रविधि) तह-८ र सहायक प्रबन्धक (सूचना प्रविधि) तह-६ पदको खुल्ला प्रतियोगितात्मक लिखित परीक्षाको पाठ्यक्रम

समय : ३ घण्टा पूर्णाङ्क:- १००

पाठ्यक्रमलाई चार खण्डमा विभाजन गरिएको छ।

खण्ड (क)

सामान्य ज्ञान र बैंकिङ्ग

- नेपालको बैकिङ्ग प्रणाली ।
- २. नेपालको भौगोलिक, सामाजिक, धार्मिक, ऐतिहासिक तथा आर्थिक विकास सम्बन्धी विविध जानकारी ।
- ३. SAARC मुलुक र नेपालका प्रमुख घटनाहरुको जानकारी ।
- ४. नेपालको संवैधानिक व्यवस्था,
- X. राष्ट्रिय तथा अन्तरराष्ट्रिय संघ∕संस्थाहरु सम्बन्धी जानकारी: World Bank, ADB, CGAP, UNDP, WTO, Grameen Bank Bangladesh, WWB, RMDC, CSD, CMF।

खण्ड (ख)

ब्यवस्थापन तथा लघ्वित्त सम्बन्धी

- १. नेपालमा लघ्वित्त कार्यक्रम।
- नेपालको गरौबी निवारणमा स्वावलम्बन लघुवित्त वित्तीय संस्था लि. को भूमिका, उपलब्धि, कमजोरीहरु, संभावना, चुनौतिहरु ।
- ३. लघ्वित्तमा केन्द्र बैठक संचालन तथा व्यवस्थापन सम्बन्धी आधारभूत जानकारी ।
- ४. कार्यालय संचालन तथा व्यवस्थापन ।

खण्ड (ग)

ऐन, नियम तथा निर्देशनहरु

सूचना प्रविधि सम्बन्धी नीति र यस सम्बन्धी प्रचलित ऐन, नियमहरु ।
सूचना प्रविधि सम्बन्धी नेपाल राष्ट्र बैंकबाट जारी निर्देशनहरु/मार्गदर्शनहरु ।

खण्ड (घ)

सूचना प्रविधि सेवा सम्बन्धी

Basic knowledge:

Applied Electronics, Digital Logic Design, Low level/High level Programming Languages, Data Structures, Computer Organization/Architecture, Operating system, DBMS, Communication & Networking, Internet/email system, new media fundamentals, computer security, ERP systems, emerging technologies, General knowledge on banking software used in Nepalese banking system **Fundamentals of Operating Systems:**

Role of Operating Systems, Introduction to different subsystems of an Operating System, Unix/Linux/Windows operating system, Abstraction and problem solving through programming, Java application development environment, Data types, variables and operators, Methods and

(अंक १० х १=१०)

(अंक २ **x** ४=१०)

(sian ? X X=90)

(अंक ७ x १०=७०)

conditional operators, Control structures: sequence, repetition and selection, Classes and Objects, Introduction to Graphical User Interface (GUI) programming, Operating System designs, Process Management & Scheduling, Deadlock Characterization & Management, Memory management, Virtual Memory, Parallelism and Pipelining with CPU

Communication & Network Technologies:

Data Transmission models, Modems and remote network access, Error detection and correction techniques, Data Compression Techniques, Network Topologies and Network Design, Networking Devices, Internet services, Internet Protocol/addressing, Network security, Network devices like routers, switches, firewalls, load balancers, Encryption/Cryptography, Digital authentication.

Concept of packet switching and Circuit Switching, Email System, Basic Concept of Internet. Data Encryption, Digital Signature.

System Administration and Management:

Server technologies and architectures, Server and client services, Server configuration and management, Application servers, administrative domains, Emerging trends. Deploying and Managing Windows Server 2019, Active Directory Domain Services, IPv4, IPv6 and Dynamic Host Configuration, Protocol, Domain Name System, File and Print Services, Group Policy, Server Virtualization with Hyper-V, Managing Risk and Disaster Recovery, Managing Quality by Monitoring Windows.

System/Enterprise Architecture:

Various System Architecture, Service Oriented Architecture and Service Design, Requirement Engineering, Reverse Engineering, Cloud Computing, Architectural Patterns, System Test Plans, Case Studies in System Architecture, Current Trends in System Architecture, EA: definitions, meaning of EA, need for EA, the context of EA: business and IT cycles, Business-IT alignment, The EA process: Align Elaborate and Govern, IT planning in the context of EA, the value of EA, Change Management.

Enterprise Network Server Administration:

Deploying and Maintaining Server Images, Advanced Network Services, DHCP and DNS, Active Directory Domain Services, Sites and Replication, Group Policy Infrastructure, Network Policy Server and Network Access Protection, Update Management, Advanced File Services, Active Directory Certificate Services, Active Directory Rights, Management Services, Active Directory Federation Services, High Availability with Network Load Balancing and Failover Clustering. Assess a secure network access strategy, configure advanced IP address management using DHCP and DNS, troubleshoot network access, Windows Server deployment and migration strategies, Manage Server role requirements, Manage Server and Data Security, Appraise a policy strategy within an Active Directory infrastructure.

Information System Security Management:

Introduction to the management of information security, planning for information security, planning for contingencies, Information Security Policy, Developing the security program, Security Management Practices, Risk Management: identifying and assessing risk, Risk Management: Assessing and controlling risk, Protection Mechanisms.

Virtual Private Networks:

Overview of VPN in security context, its characteristics, requirements, and architecture, SSL VPN protocols and configurations, Internet Key Exchange Protocol version 1 and 2, IKE v1 & 2 and ISAKMP, Site-to-Site IPsec VPN Operations, VPN routes management/handling at gateways, Overview of MPLS VPN Technology.

Networking Fundamentals:

Networking Fundamentals, OSI Network Layers, Ethernet fundamentals, technologies and switching, TCP/IP and addressing, Subnets and subnetting (VLSM and CIDR), Routing fundamentals, Static

and dynamic routing, Configuring routers and routing devices, Routing protocols (RIP, RIPv2, EIGRP, OSPF), Basic router troubleshooting.

Network Switching:

Switching Fundamentals, Technologies of switching, TCP/IP and addressing, Subnets and subnetting (VLSM and CIDR), Switching concepts, Virtual LANs, Inter-VLAN Static routing, Ether channel Bundling, Spanning Tree Protocol, Wireless LANs, Switch troubleshooting

Network Routing:

Routing fundamentals, Static and dynamic routing, Configuring routers and routing devices, Routing protocols (RIP, RIPv2, EIGRP, OSPF), WAN technologies, Access Control Lists, PPP, DHCP and NAT Services, Frame relay, Network troubleshooting

Design & Management of Networks:

Legacy Network Technologies (PSTN, ISDN, Dialup, FR, ATM, PDH, SDH, SONET), Wired Access Network Technologies (xDSL, HFC CMTS, FTTx), Wireless Access Network, Technologies (WiFi, WiMax, Microwave, Satellite, FSO), Mobile Networks Evolution, Mobile Network Technologies (3GPP, 4G LTE), Backbone Network Technologies (DWDM, MPLS, MetroEthernet), Design of Next Generation Public Access Networks – Wired and Wireless, Design of Next Generation Public Core Networks, Virtual Private Networks, Remote Access Networking, Managing Secure Access, Next Generation Service Model, Next Generation, Services (VoIP, Virtual PBX, OTT, Cloud Computing, SaaS, IaaS), QoS: Network-centric and User-Perceived, Network Management and Security, The Future of Networking: SDN

Information Systems Risk & Security:

An introduction to Information Systems risk and security, Risk management, assessment and mitigation, Information security management, governance and assurance, The role of policies and standards in IS risk and security management, Contingency planning, including incident management, business continuity and disaster recovery planning, Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring, Compliance frameworks and legal, professional and ethical issues in IS security and risk management, Major Theories, concepts and methodologies for managing information systems and assuring the integrity and security of information assets, The socio-technological dimensions (human and organizational factors) in IS security and risk management

Secure Remote Access Networks:

Modern network security threats, Securing network devices, Authentication, Authorization and Accounting, Implementing Firewall technologies, Implementing Intrusion Prevention, Securing the Local Area Network, Cryptographic System, Implementing Virtual Private Networks, Implementing ASA, Managing a Secure Network

IT Security:

Overview of Internet Crime and computer security threats, Operating System Flaws, Security Tools, System logs, Firewalls, security: theory, practice, design, Ports scanning, packet sniffing and intrusion detection, Understanding and responding to security alerts, Server technologies, risks and policies, Vulnerability analysis and Audit, Secure programming practices, Script injection and input sanitizing, Security Models, Physical Security, Authentication (identity, biometrics and digital signatures) Evaluate security of client and server computers, Plan security audits, demonstrate an understanding of the concepts of social engineering and physical security, Use a variety of security related tools, Identify attacks and mitigate attacks, Evaluate authentication and encryption systems

System/Network Security & Resilience:

Threats to overall systems/network security, Security policy, Firewalls, Encryption, Virtual Private Networks, Intrusion Detection Systems, Authentication Systems, Wireless Security etc...

