	Customer Responsibilities	Cloud Service Provider (SLT) Responsibilities
1. Shared Roles and Responsibilities in a Cloud Computing Environment (CLD.6.3.1)	1.1 Virtual Machine (VM) & Virtual Data Center (VDC) Management • For individual VMs, the Cloud Service Provider (CSP) will provision the requested OS and configure access (SSH/RDP via VPN or internet). The CSP will provide initial credentials, which the customer must change immediately upon first login. Thereafter, the customer assumes full responsibility for VM security, maintenance, and management, and the CSP shall not be liable for any issues arising thereafter. • For Virtual Data Centers (VDCs), the Cloud Service Provider (CSP) shall provision the VDC with the agreed-upon resources and provide the tenant credentials to the customer. The customer is solely responsible for provisioning, managing, and upgrading virtual machines (VMs) within their VDC. The CSP will not be involved in VM creation, resource allocation, or modifications within the VDC at any stage. • The Customer is responsible for managing and securing all individual Virtual Machines (VMs) and VMs created within their assigned Virtual Data Centers (VDCs). • The Customer must configure applications, databases, and security settings within their VMs. 1.2 Operating System and Software Security • The Customer must ensure that all operating systems and software installed on VMs are kept up to date with the latest security patches. • The Customer must implement and maintain antivirus (AV) and endpoint security solutions.	1.1 Security of Cloud Infrastructure • Maintain and secure the cloud platforms (e.g., VMware, OpenShift) to industry security standards. • Regularly patch hypervisors and virtualization infrastructure. • Ensure physical security of data centers and high availability of infrastructure. 1.2 Service Provisioning and Access Control • Provision VMs with OS, vCPU, vRAM, and storage, and share initial credentials securely. • Enforce access control policies for cloud platform administrators. • Restrict publicly exposed management interfaces to authorized personnel only. 1.3 Security Monitoring & Logging • Monitor cloud platform activities for security events and unauthorized access. • Maintain logs of administrative actions and enforce compliance with access policies. 1.4 Incident Management & Service Assurance • Respond to faults and incidents reported via tickets or helpline. • Notify customers before planned maintenance or downtime. 1.5 Data Backup & Recovery

	1.3 Data Protection and Backup • The Customer is responsible for encrypting sensitive data stored in their VMs and VDCs. • The Customer must manage and maintain backups unless they have purchased a backup service from the Cloud Service Provider (CSP). 1.4 User Access and Identity Management • The Customer must manage access credentials and enforce role-based access control (RBAC) for users accessing their VMs and applications. • Multi-Factor Authentication (MFA) is strongly recommended for administrative and privileged accounts.	• Provide a backup service as an optional offering (customers are responsible for enabling it). • CSP is not responsible for customer data loss if the backup service is not used. 1.6 Service Termination & Data Retention • Disable VMs/VDCs upon service termination and retain them for one month before deletion. • Allow customers to retrieve their data during the retention period.
2. Secure Removal of Cloud Customer Assets (CLD.8.1.5)	2.1 Data Backup and Retention Before Termination • The Customer must take backups of their data before requesting service termination. • If the Customer has purchased the CSP's backup service, they must restore their data before permanent deletion. 2.2 Secure Data Deletion from VMs/VDCs • Before termination, the Customer must securely erase or encrypt sensitive data to prevent unauthorized access. • The Customer should use secure deletion tools or encryption methods to protect residual data. 2.3 Access Revocation and Service Decommissioning	2.1 Secure Data Deletion • After the one-month grace period, permanently delete customer VMs/VDCs. • Ensure secure deletion methods 2.2 Prevent Unauthorized Access to Decommissioned Resources • Restrict access to deactivated VMs during the retention period. • Remove any CSP-managed credentials associated with terminated resources. 2.3 Audit and Compliance Logging • Maintain logs of asset decommissioning, including timestamps and deletion confirmations.

	• The Customer must decommission user access to their applications running in the cloud before service termination. • Third-party integrations must be disabled before VM/VDC deletion. 2.4 Compliance with Data Protection Regulations • The Customer is responsible for ensuring compliance with internal policies, industry standards, and regulatory requirements when decommissioning cloud resources.	• Keep audit trails for compliance and future reference.
3. Segregation in Virtual Computing Environments (CLD.9.5.1)	3.1 Secure Configuration of Virtual Machines and VDCs • The Customer must configure their VMs and applications to prevent unauthorized access. • The Customer should implement network segmentation within their VDCs (e.g., separate production and development environments). 3.2 Data Protection and Encryption • The Customer must encrypt sensitive data within VMs to protect against unauthorized access. • File system and database-level encryption are strongly recommended. 3.3 Network Security Measures • The Customer must configure firewalls within VMs and VDCs to restrict access to authorized IPs only. • Proper segmentation between internal services must be maintained to prevent lateral movement in case of a breach.	3. Segregation in Virtual Computing Environments (CLD.9.5.1) 3.1 Isolation of Customer Environments • Ensure that customer VMs are logically and network-wise isolated from other tenants. • Use VLANs, SDN, and firewall rules to enforce multi-tenancy security. 3.2 Security Monitoring & Compliance • Monitor for misconfigurations that could lead to data leakage or unauthorized access. • Conduct regular security assessments to ensure compliance with segregation policies. 3.3 Role-Based Access for CSP Operations • Implement Privileged Access Management (PAM) to secure administrative access. • Restrict CSP administrator access to customer environments only upon approval.

4. Virtual Machine Hardening (CLD.9.5.2)	4.1 OS Hardening & Security Configurations • The Customer must apply security baselines (e.g., CIS Benchmarks, vendor security guides) to harden OS configurations. • The Customer must disable unnecessary services, ports, and accounts on VMs. 4.2 Patch Management & Vulnerability Remediation • The Customer must regularly update their operating systems and applications to address security vulnerabilities. • Vulnerability assessments (VA) should be conducted to identify and mitigate risks. 4.3 Access Control & Identity Management • The Customer must enforce least privilege access and use role-based access control (RBAC) for VM administrators. • Multi-Factor Authentication (MFA) is strongly recommended. 4.4 Network Security and Monitoring • The Customer must implement host-based firewalls and restrict remote access (SSH/RDP) to trusted IPs only. • Security monitoring and logging must be enabled on all VMs.	4.1 Secure VM Deployment • Provide pre-configured hardened OS images with essential security patches. • Regularly update VM templates to address new vulnerabilities. 4.2 Network & Access Security • Maintain secure hypervisor configurations to protect against exploits. • Use firewall rules and VLANs to prevent unauthorized cross-tenant access. 4.3 Security Monitoring & Threat Detection • Monitor cloud infrastructure for security incidents and suspicious activities. • Provide logs or alerts to customers if malicious activity is detected. 4.4 Secure VM Decommissioning • Retain disabled VMs for one month, then securely delete them. • Ensure data sanitization before reusing storage resources.
5. Administrator's Operational Security (CLD.12.1.5)	5.1 Secure Administrative Access • The Customer must enforce role-based access control (RBAC) for VM and application administrators.	5.1 Secure Administrative Access • Implement Privileged Access Management (PAM) for secure admin authentication.

	• The least privilege principle must be followed to minimize exposure to critical systems. 5.2 Credential and Password Management • The Customer must rotate administrator credentials regularly and enforce strong password policies. • Shared admin accounts must be avoided to maintain accountability. 5.3 Monitoring and Logging of Admin Activities • The Customer must enable logging and monitoring of administrative actions on VMs and applications. • Regular log reviews should be conducted to detect suspicious activity. 5.4 Secure Remote Administration • The Customer must restrict remote admin access to trusted IP addresses. • Secure protocols such as SSH key-based authentication and RDP Network Level Authentication (NLA) should be used.	• Restrict CSP admin access to customer environments only for support purposes. • Enforce Multi-Factor Authentication (MFA) for CSP administrators. 5.2 Logging & Monitoring of CSP Admin Actions • Log all CSP administrator actions related to customer environments. • Ensure logs are tamper-proof and retained for compliance. 5.3 Infrastructure Patching & Hardening • Regularly patch virtualization platforms (VMware, OpenShift) to fix vulnerabilities. • Apply industry best practices to secure cloud infrastructure components. 5.4 Secure Communication of Credentials • Move towards secure credential management (e.g., password vaults, temporary credentials). • Improve current credential-sharing methods (e.g., avoid email-based sharing).
6. Monitoring of Cloud Services (CLD.12.4.5)	6.1 Performance Monitoring of VMs and Applications • The Customer must monitor resource usage, system health, and uptime to detect performance issues. • Logs, alerts, and dashboards should be utilized for proactive monitoring. 6.2 Security Event Monitoring	6.1 Infrastructure & Platform Monitoring • Continuously monitor cloud infrastructure health, performance, and resource utilization. • Detect and respond to performance bottlenecks and security incidents. 6.2 Network & Security Monitoring

	• The Customer must enable logging of security-related events, including failed logins and privilege escalation attempts. • Security Information and Event Management (SIEM) systems should be used for centralized log analysis. 6.3 Patching and Vulnerability Management • The Customer must apply security patches regularly to reduce security risks. • Vulnerability scanning tools should be used to detect and address system weaknesses. 6.4 Backup and Data Integrity Monitoring • The Customer must verify backup processes and ensure that backup data remains intact. • Regular backup integrity tests should be performed.	• Implement intrusion detection and prevention systems (IDS/IPS). • Monitor network traffic for unusual activity or attacks. 6.3 Security Logging & Incident Response • Log all CSP administrative actions on the platform. • Investigate and respond to security incidents affecting multiple customers. 6.4 Service Level Agreement (SLA) Compliance • Ensure uptime and availability as per SLAs (if applicable). • Notify customers about planned and unplanned service outages.
7. Alignment of security management for virtual and physical networks (CLD.13.1.4)	7.1 VM and Application Network Security • The Customer must configure firewall rules, security groups, and network segmentation to limit access. • Host-based security controls (e.g., iptables, Windows Firewall) should be used where applicable. 7.2 Network Access Controls • The Customer must restrict SSH/RDP access based on least privilege principles. • Network configurations should be reviewed regularly for security compliance. 7.3 Patch Management for Network Components in VMs	7.1 Data Center & Network Security • Secure physical network infrastructure (e.g., firewalls, routers, switches). • Implement DDoS protection and network intrusion detection. • Ensure customer traffic is isolated to prevent cross-tenant attacks. 7.2 Segmentation of Virtual Networks (VDCs & Containers) • Enforce strong access controls for virtual networks (VDC, Kubernetes, and containers). • Restrict public-facing access to admin consoles (e.g., OpenShift, vCloud Director).

	• The Customer must update OS and network-related components (e.g., OpenSSH, VPN software) regularly. • Vulnerability scans should be conducted to detect outdated network configurations. 7.4 Compliance with CSP's Network Security Policies • The Customer must follow the CSP's security guidelines for segmentation, access control, and secure network practices. • Compliance with security best practices is required when configuring network services inside the cloud. 7.5 Business Continuity & Disaster Recovery • The Customer must establish redundancy, and failover plans for applications running on VMs/VDCs. • Disaster recovery mechanisms should be tested regularly.	7.3 Security Monitoring & Incident Response • Monitor network traffic at the hypervisor level for threats. • Investigate and respond to network-related security incidents. 7.4 Network Security Best Practices for Customers • Provide security guidelines for VM networking, firewall configurations, and segmentation. • Offer recommendations for VPN usage, encryption, and best practices. 7.5 Service Availability & Load Balancing • Ensure network redundancy to minimize service disruptions. • Improve failover processes to enhance cloud service resilience.
8. PII Compliance	• Provide accurate administrator contact information (email/phone). • Do not share unnecessary personal data with CSP • Reset all default credentials immediately after access. Restrict VM access to authorized personnel. • Notify CSP of administrator changes promptly. • Monitor VMs for suspicious activity. Report VM security incidents to CSP within 72 hours. • Remove all sensitive data from VMs before termination.	• Communicate how customer contact details are used (account setup/support only). Never uses customer data for advertising. • Only collects necessary details (admin name/email). Never requests sensitive IDs (passports, etc.). • Encrypts customer contact details (OSS). Provides temporary VM credentials (expire after first use). • Maintains up-to-date contacts when notified (AM updates vis CRM) • Notifies customer within 72 hours of contact data breaches. Addresses CSP-side vulnerabilities.

	• Approve/reject subcontractors per contract terms. • Specify permitted/disallowed data locations. • Full responsibility for OS/application maintenance, patching, performance monitoring and troubleshooting. Must manage all VM credentials without CSP involvement. • It is the responsibility of the customer to execute remediation actions (ex. Restart VMs, Scale resources, Apply patches)	• Notifies customer within 72 hours of contact data breaches. Addresses CSP-side vulnerabilities. • Discloses all subcontractors handling customer data. Requires subcontractor compliance. • Discloses data storage jurisdictions. • Under no circumstances will CSP personnel log into customer VMs • Only involved in providing non-intrusive recommendations (ex. VM is at 95% memory utilization) in cases where customer lodge a complaint.