**Տեխնիկական բնութագիր\***

ամպային հաշվողական ռեսուրսների, Microsoft Windows արտոնագրերի, տվյալների պահոցի, տվյալների հոսքի կապուղու, համացանցի, հրեպատի և պահեստային ծառայությունների ձեռքբերման

**Հաշվողական ռեսուրսներ, ներառյալ Windows 2022(կամ ավելի բարձր) հավաստագրեր Windows վիրտուալ մեքենաների համար, նշված քանակի և vCPU-ների համար**

| OS | vCPU | RAM, Gb | Storage1, Gb | Storage2,Gb | Storage3,Gb | Net Gb/sec |
| --- | --- | --- | --- | --- | --- | --- |
| Windows Server Std 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Std 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Std 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Std 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Std 2022+ | 8 | 48 | 100 | 150 | 2500+ | 1+ |
| Windows Server Std 2022+ | 8 | 48 | 100 | 150 | 2500+ | 1+ |
| Windows Server Std 2022+ | 2 | 4 | 100 |  |  | 1+ |
| Windows Server Std 2022+ | 6 | 24 | 100 |  |  | 1+ |
| Windows Server Std 2022+ | 6 | 24 | 100 |  |  | 1+ |
| Linux platform | 2 | 2 | 100 |  |  | 1+ |

**Համացանցի ծառայության նկատմամբ պահանջներ, տեխնիկական նկարագրություն**

| **Category** | **Requirement** | **Parameter/Metric** | **Target /Value** |
| --- | --- | --- | --- |
| Service Type | CIR Internet access | Service type | Business/enterprise CIR Internet |
| Service Type | Delivery site | Installation location | CSP DC rack (Exchange/AD/NGFW) |
| Bandwidth | Committed symmetric bandwidth | CIR Up/Down | ≥ 100 Mbit/s / 100 Mbit/s, full duplex |
| Bandwidth | Pay-as-you-go scalability | Upgrade/downgrade | On-demand increase/decrease above/below 100/100 |
| Bandwidth | PAYG billing method | Usage accounting | Simple tiered PAYG (preferred) or 95th percentile |
| Bandwidth | No shaping below CIR | Shaping / policing | No shaping/policing below CIR (except agreed DDoS mitigation) |
| Availability | Service availability | Availability | ≥ 99.9% per calendar year |
| Availability | Outage definition | Loss threshold | Packet loss ≥ 50% for > 1 minute = outage |
| Maintenance | Planned maintenance notice | Notice period | ≥ 5 working days |
| Maintenance | Maintenance window timing | Time of day | Outside business hours (00:00–06:00 local) |
| Maintenance | Planned maintenance cap | Total per month | ≤ 8 hours/month |
| Performance | Latency | RTT 95th percentile | ≤ 20 ms to ISP upstream/peering |
| Performance | Jitter | 95th percentile | ≤ 10 ms |
| Performance | Packet loss | Monthly average | ≤ 0.1% (excluding outages & maintenance) |
| Throughput | Usable IP throughput | Goodput vs CIR | ≥ 90% of CIR |
| Routing/IP | Public IP addressing | Static IPv4 allocation | /29 public IPv4 subnet (5 usable IPs) |
| Routing/IP | No carrier NAT | NAT policy | No CGNAT (must be publicly routable) |
| Security | DDoS protection | Volumetric mitigation | Included |
| Security | Port neutrality | Allowed ports/protocols | No blocking of required ports |
| Support | NOC coverage | Support hours | 24/7/365 |
| Support | Fault response time | Response | ≤ 15 minutes from detection/ticket |
| Support | Restoration time (critical) | MTTR | ≤ 4 hours for total outage/severe degradation |
| Monitoring & Reporting | Customer visibility | Portal / reports | Portal/API or monthly SLA report |
| Remedies | Service credits | Credit schedule | Defined credit table |
| Remedies | Chronic breach termination | Exit clause | Right to terminate after repeated SLA breaches |

**Հաջորդ սերնդի հրեպատի նկատմամբ պահանջներ (սարքավորում կամ համապատասխան virtual appliance)՝**

| Spec | Class B |
| --- | --- |
| Typical use | Large Branch/Regional HQ (≤500 users, stackable) |
| FW IMIX throughput (Gbps) measured per RFC 3511/2647 | ≥8 |
| Threat prevention w/ full L7 (Gbps) | ≥5 |
| New sessions per second | ≥100k |
| Max concurrent sessions | ≥4M |
| Stateful FW, NAT, zones, IPv4/IPv6 dual-stack | Required |
| DPI (L7 App-ID / signature + heuristics) | Required |
| IPS (NGIPS) | Required |
| WAF (integrated reverse-proxy or tightly integrated module; OWASP CRS-compatible ruleset) | Required |
| Advanced malware detection (ML/AV) | Required |
| Sandboxing | On-prem required |
| Cloud sandbox | Not-required. If offered: MUST encrypt in transit/at rest, provide DPA, GDPR-aligned data handling, regional data residency, and ISO/IEC 27001/SOC 2 attestation. |
| TLS 1.3 decryption (fwd proxy & inbound reverse) | Required |
| Zero-Trust (NIST SP 800-207 alignment; ZTNA policy enforcement point; per-session authZ) | Required |
| Identity awareness (AD/Azure AD/LDAP; user-ID mapping) | Required |
| Admin SSO (SAML 2.0 / OpenID Connect) | Required |
| Dynamic path selection / steering by app & SLA (MEF 70.1/70.2 attributes) | Required |
| Underlay/overlay: IPsec (ESP) with IKEv2; TLS-based tunnels | Required |
| Performance probes (jitter/latency/loss), BFD single-hop | Required |
| MPLS/BGP/OSPF/Static; ECMP | Required |
| VoIP protections (SIP ALG toggle, DSCP preserve/remark) | Required |
| Exchange Online Protection-comparable mail security integration for hybrid flows: SPF/DKIM/DMARC validation; SMTP TLS/mTLS enforcement; connector interop; attachment detonation; URL rewrite/time-of-click equivalent; header/stamp preservation for traceability | Required |
| HA (stateful A/S) | Required; ≤1s |
| Clustering / stacking (single admin domain, policy sync, unified logs) | Required (≥2 nodes) |
| Virtual systems (multi-tenant contexts) | Not-required |
| GE copper (RJ-45) | ≥12 |
| SFP/SFP+ 1/10G | ≥6 SFP+ |
| 25G SFP28 | Not-required. If offered: must interop per IEEE 802.3ba/bs. |
| 40/100G (QSFP+/QSFP28) | Not-required. If offered: must interop per IEEE 802.3ba/bs. |
| Console/USB | RJ-45/USB-C |
| Local GUI/CLI; SSHv2; role-based admin | Required |
| APIs (REST/NETCONF); Ansible-friendly | Required |
| Syslog structured (RFC 5424) & TLS syslog (RFC 5425) to SIEM; IPFIX or NetFlow export (RFC 7011/compatible) | Required |
| NTPv4 time sync | Required |
| SNMPv3 | Required |
| AC input | 100–240V AC |
| Plug / cable in box | Type F (Schuko) |
| Operating temp (°C) | 0…45 |
| Rack kit | Required (1U/2U as applicable) |
| Noise (dBA @25°C) | ≤55 |
| Power cable | 2× Type-F (if dual PSU) |
| Earthing accessories | Protective earthing required; earthing accessories Included (earthing cable/lug/screws) |
| Patch cords | 4× Cat6a (≥2 m) |
| High-speed interconnects | Include 4× SFP+ DAC (≤3 m) |
| Licenses included | 60-month subscriptions covering: IPS, URL filtering, AV/AM, identity, SD-WAN, centralized mgmt, log forwarding, TLS decryption/WAF/sandbox |
| Sandbox license | On-prem engine license included (60 mo) |
| Software support | Security updates & feature releases for ≥5 years from acceptance |
| HW warranty | ≥3 years NBD advance replacement |
| Documentation | Admin + hardening guide + MIB/API references |

**Data link ծառայություն ՀՀ Բարձր տեխնոլգիական արդյունաբերության նախարարության՝ Վազգեն Սարգսյան 3, ք. Երևան և ՏՄԿ միջև՝**

| **Category** | **Requirement** | **Parameter / Metric** | **Target / Value** |
| --- | --- | --- | --- |
| Service Type | L2 point-to-point service | Service type | Layer 2 Ethernet (e.g. EoMPLS / EVPN / equivalent) |
| Service Type | Endpoints | A-end / B-end | CSP DC rack (Exchange/AD/NGFW) ↔ Government office core (addr: Vazgen Sargsyan 3, Yerevan) |
| Bandwidth | Committed symmetric bandwidth | CIR | ≥ 100 Mbit/s up & down, full duplex |
| Bandwidth | No shaping below CIR | Shaping / policing | No shaping/policing below CIR (except agreed DoS protection) |
| L2 Characteristics | Ethernet framing | Standard | IEEE 802.3 Ethernet |
| L2 Characteristics | VLAN support | Tagging | IEEE 802.1Q VLAN tagging supported; QinQ (802.1ad) if requested |
| L2 Characteristics | MTU | Effective IP MTU | ≥ 1500 bytes IP payload without fragmentation |
| Redundancy | Path diversity (if ordered) | Physical / logical paths | Two diverse paths & independent last-mile (where feasible) |
| Availability | Annual service availability | Availability | ≥ 99,9% per calendar year |
| Availability | Unavailability definition | Loss threshold | Packet loss ≥ 50% for > 1 minute = outage |
| Maintenance | Planned maintenance notice | Notice period | ≥ 5 working days before maintenance |
| Maintenance | Maintenance window timing | Time of day | Outside business hours (e.g. 00:00–06:00 local) |
| Maintenance | Maintenance duration cap | Total per month | ≤ 8 hours/month planned maintenance |
| Latency | One-way latency | 95th percentile | ≤ 10 ms (office ↔ CSP) |
| Jitter | Packet delay variation | 95th percentile | ≤ 5 ms |
| Packet Loss | Average packet loss | Monthly average | ≤ 0.1% (excluding outages & maintenance) |
| Throughput | Usable IP throughput | Goodput vs CIR | ≥ 90% of CIR (e.g. ≥ 90 Mbit/s IP payload for 100 Mbit/s service) |
| Support | Fault response time | Response | ≤ 15 minutes from detection or ticket opening |
| Support | Restoration time – critical | Outage restoration | ≤ 4 hours for total outage / severe degradation during business hours |
| Support | Restoration time – major degradation | Degradation fix | ≤ 8 hours for SLA breach without full outage |
| QoS | DSCP transparency | DSCP handling | Preserve DiffServ / DSCP markings; no default remarking |
| QoS | 802.1p transparency | CoS bits | Preserve 802.1p CoS bits in tagged frames |
| QoS | No oversubscription below CIR | Congestion | No provider congestion-induced drops up to CIR |
| Provider Monitoring | 24×7 monitoring | NOC coverage | 24×7 monitoring of link state and metrics |
| Provider Monitoring | Probing frequency | Probe interval | ≥ 1 probe/sec for availability/loss/latency/jitter |
| Provider Monitoring | Alarm thresholds – loss | Loss trigger | Alarm if loss > 1% for > 5 consecutive minutes |
| Provider Monitoring | Alarm thresholds – latency | Latency trigger | Alarm if latency > 2× SLA (e.g. > 20 ms) for > 5 min |
| Provider Monitoring | Alarm thresholds – jitter | Jitter trigger | Alarm if jitter > 2× SLA (e.g. > 10 ms) for > 5 min |
| Provider Portal | Customer portal / API | Visibility | Web portal or API with near real-time (≤ 5 min delay) status |
| Provider Portal | Historical data retention | Retention period | ≥ 365 days of history (utilization, latency, jitter, loss, outages) |
| Reporting | Monthly SLA reports | Report scope | Monthly report with availability, latency, jitter, loss, incidents, maintenance |
| Customer Monitoring | Active probes allowed | Probe traffic | Customer may run ICMP/UDP/TWAMP probes without blocking (within reasonable volume) |
| Customer Monitoring | CPE telemetry | Stats sharing | If provider CPE is used as demarc, SNMPv3 or telemetry access to basic interface stats |
| Customer Monitoring | Utilization alert – warning | Threshold | Alert if > 70% CIR for > 10 minutes |
| Customer Monitoring | Utilization alert – critical | Threshold | Alert if > 90% CIR for > 5 minutes |
| Customer Monitoring | Quality alerts | Thresholds | Alerts if loss > 1%, latency > 10 ms, jitter > 5 ms for > 5 minutes |
| Demarcation | Demarc definition | Demarc points | Clear A-end and B-end demarc (NID/switch ports) in contract and RFS docs |
| Demarcation | Handover interface | Physical interface | Electrical or optical Ethernet (e.g. 1000BASE-T or 1000BASE-SX/LX, or higher) |
| Demarcation | Optics responsibility | SFP/SFP+ | Provider supplies necessary SFP/SFP+ or media converters unless otherwise agreed |
| Security | Logical isolation | VPN / instance | Traffic carried in dedicated MPLS VPN / EVPN / VPLS or equivalent isolated instance |
| Security | Privacy of payload | Payload handling | Provider shall not mirror or inspect payload except for DDoS protection or troubleshooting on request |
| Security | Secure management of CPE | Mgmt protocols | Only secure protocols (SSH, SNMPv3, HTTPS/TLS) for managing provider demarc devices |

**Տվյալների պահեստավորման ծառայության նկատմամբ տեխնիկական պահանջներ**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Requirement** | **Parameter/Metric** | **Target /Value** |
| Backup | Managed backup service (production) | Service scope | Provider-managed, application-consistent backups for all virtual machines supporting service configurations. |
| Backup | Backup schedule | RPO | ≤ 24 hours (daily backups) |
| Backup | Restore capability | RTO (target) | Restore test available on request; critical restore ≤ 8 hours |
| Backup | Retention | Retention period | ≥ 30 days (base) |
| Backup | Backup storage protection | Immutability | Immutability or equivalent tamper protection for backup copies |
| Backup | Backup encryption | Encryption | Encryption in transit and at rest |
| Backup | Backup reporting | Reporting | Monthly backup report (success rate, protected assets, restore points, storage used) |
| Backup | Pay-as-you-go billing | Billing model | Pay-as-you-go based on protected capacity (GB/TB) and/or number of protected workloads |
| Backup | PAYG scaling | Add/remove protected assets | On-demand enable/disable per server/workload |
| Backup | Access & restore request process | Operations | 24/7 restore request channel; restore initiated within agreed response time |

Կատարողը պարտավոր է ապահովել վերը նշված ծառայությունների և հաշվողական ռեսուրսների տրամադրումը «Ըստ պահանջի» (On-Demand) ընդլայնման հնարավորության մոդելով՝ համակարգը նախագծելով և շահագործելով այնպես, որ ապահովվի հաշվարկային բեռնվածության տարեկան միջինում առնվազն 10 % աճի աջակցումը՝ առանց ծառայությունների որակի խաթարման։

Վճարումները պետք է իրականացվեն «Վճարիր ըստ օգտագործման» (Pay-As-You-Go) հաշվարկման մոդելով՝ պայմանով, որ Կատարողը յուրաքանչյուր հաշվետու ամսվա համար ներկայացնի հաշիվ-ապրանքագիր՝ ներառելով փաստացի օգտագործված հաշվարկային ռեսուրսների (հաշվողական միավորներ, ծավալներ և այլ համապատասխան չափանիշներ) մանրամասն և թափանցիկ բացվածքը (մանրամասն պահանջները՝ ՏՄԿ բաժնում)։

**Տվյալների մշակման կենտրոնի (ՏՄԿ) նկատմամբ պահանջներ՝**

**Տվյալների կենտրոնի նկատմամբ պահանջներ**

1. Կատարողը Պատվիրատուին տրամադրում է ՏՄԿ ենթակառուցվածքում պետական սեկտորի համար առանձնացված սերվերներ։
2. ՏՄԿ ենթակառուցվածքը պետք է ապահովված լինի էլեկտրասնուցման համակարգով, որն առնվազն պետք է պարունակի՝ լիովին իրարից անկախ սնուցման աղբյուրներ (առնվազն 2 գիծ տարբեր ենթակայաններից, որոնք տվյալների կենտրոնին միանում են տարբեր` իրար չզուգակցող ճանապարհներով), պահուստային դիզելային գեներատորներ, որոնցից յուրաքանչյուրի հզորությունը պետք է բավարարի և ապահովի ամբողջ կենտրոնի էլեկտրամատակարարումը հիմնական 2 էլեկտրասնուցման աղբյուրների իսպառ բացակայության պայմաններում, անխափան սնուցման աղբյուրներ (UPS)՝ պահուստավորմամբ, պահուստային աղբյուրների ինքնաշխատ միացման ենթահամակարգ, էլեկտրասնուցման վերահսկման և կառավարման ենթահամակարգ:
3. ՏՄԿ ենթակառուցվածքը պետք է ապահովված լինիառնվազն երկու անկախհովացման համակարգերով,որոնք առնվազն պետք է ներառեն օդափոխման, սառեցման, ջերմաստիճանի և խոնավության վերահսկման համակարգեր՝ կանխելու սաքավորումների գերտաքացումն ու անջատումը։ Հովացման համակարգի հզորությունը պետք է համապատասխանի օգտագործված էներգիայի հզորությանը, իսկ սնուցումը պետք է ապահովվի տարբեր աղբյուրներից։
4. ՏՄԿ-ում օդի կայուն ջերմաստիճանը պետք է լինի 20-22°C միջակայքում (համապատասխանում է ASHRAE ստանդարտում նշված միջակայքին), իսկ օդի հարաբերական խոնավությունը՝ 40-60%:
5. ՏՄԿ ենթակառուցվածքում պետք է ապահովված լինիհեռահաղորդակցության համակարգ,որն առնվազն պետք է ներառի և ապահովի երկու և ավելի մատակարարներից անկախ՝ իրար հետ չհատվող (նույն կետը չկիսող, առանց ընդհանուր հենասյան) մալուխներով կապուղիներ տարբեր ուղղություններից, բարձր թողունակությամբ տվյալների փոխանցման գծեր, ցանցային սարքավորումներ, քրոս-միացման սենյակ, առնվազն 3 հիմնական օպերատորների առկայության հնարավորություն:
6. Կատարողը պետք է ապահովի առանձնացված (dedicated) կապուղի Պատվիրատուի գրասենյակից կամ տեղային միջավայրից դեպի ՏՄԿ։
7. ՏՄԿ ենթակառուցվածքում պետք է ապահովված լինիառնվազն երկուհրդեհային անվտանգության համակարգեր, որոնք առնվազն պետք է ներառեն և ապահովեն ծխի վաղ հայտնաբերման ենթահամակարգ, գազային կամ վակումային հրդեհաշիջման ենթահամակարգ, հրդեհային ազդարարման ավտոմատ համակարգ, մալուխային ուղիների մեկուսացում և հրդեհակայուն նյութերի կիրառում: Հրդեհային անվտանգության համակարգը պետք է համապատասխանի SP 5.13130.2009 (Systems of fire protection. Automatic fire-extinguishing and alarm systems. Designing and regulations rules) և SP 9.13130.2009 (Fire engineering. Fire extinguishers. Requirements to operation) ստանդարտերին:
8. ՏՄԿ ենթակառուցվածքում պետք է ապահովված լինի սերվերների և դրանց բաղադրիչների (օրինակ՝ էլեկտրասնուցման գծերի) N+1 պահուստավորում։
9. Պահուստային բաղադրիչ ունեցող ցանկացած հիմնական համակարգի անսարքության, շարքից դուրս գալու կամ սպասարկման/փոխարինման նպատակով անջատվելու դեպքմ պետք է գործարկվի պահուստային համակարգը և շարունակի աշխատել այնքան ժամանակ, մինչև հիմնական համակարգը վերականգնվի և դառնա աշխատունակ։
10. ՏՄԿ ենթակառուցվածքում պետք է ապահովված լինիֆիզիկական անվտանգության ապահովման համակարգ**,** որը պետք է ներառի**․**
    * մուտքի բազմամակարդակ վերահսկման և կառավարման ենթահամակարգ (բիոմետրիա, մուտքի թույլտվության քարտեր և այլն),
    * ֆիզիկական մուտքերի/ելքերի և պատուհանների կենտրոնացված կառավարման և լոգավորման ենթահամակարգ: Լոգավորման ենթակա տվյալների ցանկը պետք է ներառի առնվազն հետևյալ տեղեկատվությունը․
      + աշխատակցի/այցելուի անուն ազգանուն,
      + հասանելիության գործիքը (օրինակ՝ բեյջ, բիոմետրիկ սկանավորում, քարտ և այլն),
      + հասանելիության գործիքի նույնականացման համար,
      + աշխատակցի/այցելուի կողմից օգտագործված կոնկրետ մուտքը/ելքը,
      + անձը հաստատող փաստաթղթի տվյալներ,
      + մուտքի և ելքի ամսաթիվ, ժամ, րոպե, վայրկյան,
      + հասանելիության տրամադրման կամ մերժման վերաբերյալ նշում,
      + մերժման դեպքում՝ պատճառի մասին նշում,
      + մուտքի նպատակի կարճ նկարագրություն։

Լոգավորման ենթակա տվյալները պետք է պահպանվեն առվազն 90 օր և փոխանցվեն Պատվիրատուին ամբողջական, համաձայն վերջինիս հարցման։

* + 24/7 տեսահսկման ենթահամակարգ՝, որը պետք է ապահովի տեսադիտարկում ՏՄԿ բոլոր հատվածներում՝ առանց «կույր» գոտիների։ Տեսագրությունները պետք է պահպանվեն ամբողջ ծավալով՝ առնվազն 90 օր։ Սերվերային Պահարանի վարձակալման դեպքում Պատվիրատուին պետք է տրամադրվի վիդեոտեսահսկման ծառայությունից 24/7 ռեժիմով օգտվելու հնարավորություն։ Սերվերային Պահարանի տեսագրությունների պահպանման ժամկետը պետք է սահմանվեն պատվիրատուի պահանջի համաձայն։
  + Անվտանգության համակարգը պետք է ապահովի պարագծային պաշտպանության ենթահամակարգ (պարիսպներ, անցակետեր տուրնիկետներ, անվտանգության աշխատակիցներ)։
  + Տվայլների կենտրոնը և իր պաշտպանության պարագիծը պետք է կահավորված լինեն տվիչներով, որոնք թույլ կտան հայտնաբերել՝ շարժումը, դռների և պատուհանների չարտոնված բացումը, պատուհանների վնասումը, ոչ փակ դռներն ու պատուհանները, ինչպես նաև ծանուցել (SMS, էլ․ փոստ և այլն) համապատասխան աշխատակիցներին:
  + Անվտանգության համակարգը պետք է թույլ տա մեկ կետից տվյալների կենտրոնը բերել պահպանության ռեժիմի: Պահպանության ռեժիմը ենթադրում է անվտանգության համակարգի հատուկ գործառնական վիճակի մեկնարկ, երբ հայտնաբերվում է ֆիզիկական անվտանգությանը սպառնացող միջադեպ: Անվտանգության համակարգի պահպանության ռեժիմի ակտիվացման դեպքում պետք է գործարկվեն առնվազն հետևյալ պաշտպանական միջոցները՝
    - կենտրոնացված ծանուցումներ ուղարկում միջադեպի արձագանքման համար պատասխանատու անձանց (օրինակ՝ ֆիզիկական անվտանգության խմբին), ղեկավարությանը և այլն,
    - լրացուցիչ տեսախցիկների և տվիչների ավտոմատ ակտիվացում,
    - ֆիզիկական անվտանգության խմբի տեղակայում,
    - վտանգավոր գոտիների արգելափակում՝ նախնական գնահատման առկայության դեպքում,
    - բոլոր արտաքին և ներքին դռների արգելափակում՝ նախնական գնահատման բացակայության դեպքում,
    - հասանելիության գործիքների (օրինակ՝ բեյջ, բիոմետրիկ սկանավորում, քարտ և այլն) սահմանափակում՝ անձնակազմի ավելի փոքր խմբի համար,
    - Ոչ կրիտիկական գործողությունների (օրինակ՝ առօրյա պահուստավորման և արխիվացման գործընթացներ, առօրյա տեխնիկական սպասարկում և թեստավորումներ, պարբերական տվյալների մշակում (օրինակ՝ վերլուծական հաշվետվությունների պատրաստման նպատակով), ներքին և արտաքին համագործակցության գործիքների գործունեություն, ոչ կրիտիկական անձնակազմի մուտք համակարգ) սահմանափակում կամ կասեցում։
  + Անվտանգության համակարգը պետք է ապահովի 24/7 մշտադիտարկման և կառավարման համակարգ**,** որն առնվազն պետք է պարունակի և ապահովի՝ տվյալների կենտրոնի ենթակառուցվածքի կառավարման ենթահամակարգ, էներգիայի սպառման, հովացման ջերմաստիճանի և խոնավության մշտադիտարկման ենթահամակարգ, ջրի հայտնաբերման և տարածման կանխման համակարգ, արտակարգ իրավիճակների ծանուցման ենթահամակարգ (SMS, էլ․ փոստ և այլն)։ Մշտադիտարկման տվյալները պետք է պահպանվեն առնվազն երեք տարի ժամկետով,
  + Կատարողն՝ իր կազմակերպչական, տեխնիկական և տեխնոլոգիական միջոցներով կամ երրորդ անձի ներգրավմամբ, պետք է ապահովի ՏՄԿ տարածքի անվտանգության պահպանման ռեժիմը, որն պետք է ներառի․
    - ՏՄԿ այցելության և աշխատանքների իրականացման կարգը,
    - սարքավորումների մուտքի և ելքի կարգը,
    - Պատվիրատուի և Կատարողի աշխատակիցների դերերը և իրավասությունների մակարդակները,
  + ՏՄԿ և դրա ենթակառուցվածքներին մշտական և ժամանակավոր մուտքի (և՛ ֆիզիկական, և՛ ոչ ֆիզիկական) թուլտվություն ունեցող բոլոր անձինք (Կատարողի և պատվիրատուների աշխատակիցները) պետք է ենթարկվեն կենսագրական տվյալների ստուգումների (background checks), ներառյալ․
    - ինքնության ստուգումներ (օրինակ՝ անձնագրեր),
    - մասնագիտական համապատասխանության ստուգումներ (օրինակ՝ աշխատանքի վայրից տեղեկանք կամ սերտիֆիկատ),
    - քրեական ստուգումներ (օրինակ՝ դատվածության և հետախուզման առկայության մասին տեղեկանք)։
  + Կատարողի համապատասխան ստորաբաժանման կողմից պաշտոնական թույլտվության բացակայության դեպքում դեպի ծառայության ենթակառուցվածք չարտոնված անձնակազմի մուտքն արգելված է։ Այնուամենայնիվ, Պատվիրատուի համապատասխան աշխատակցին(ներին) տրվում է ՏՄԿ մուտք գործելու թույլտվություն՝ անհապաղ միջամտություն պահանջող արտակարգ իրավիճակներում, հետևյալ պայմաններով՝
    - Պատվիրատուն պետք է ծանուցի Կատարողին դեպի ՏՄԿ մուտքի նախաձեռնումից անմիջապես հետո։ ՏՄԿ մուտքի նախաձեռնման և դրա մասին ծանուցման իրավասությունը տրվում է հստակ անձի։ Անհրաժեշտ է ներառել վերջինիս անունը ազգանունը, անձնագրային տվյալները, հեռախոսահամար, Էլ.փոստը։
    - Կատարողի համապատասխան ստորաբաժանման լիազորված աշխատակիցը պետք է հաստատի մուտքը թույտվության հայտի միջոցով՝ արտակարգ իրավիճակի մասին ծանուցվելուց առավելագույնը 30 րոպեի ընթացքում,Կատարողի պահանջով Պատվիատուի համապատասխան աշխատակցին կարող է կցվել ուղեկցող։

1. Կատարողը՝ իր կազմակերպչական, տեխնիկական և տեխնոլոգիական միջոցներով կամ երրորդ կողմի ներգրավմամբ, պետք է ապահովի 24/7 տեղեկատվական անվտանգության շարունակական գործընթաց, որն առնվազն պետք է ներառի․
   1. միջադեպերի կանխարգելում, խոցելիությունների որոնում, հակազդող միջոցների կիրառում,
   2. 24/7 մոնիթորինգ, կիբեռհարձակումների հնարավոր դեպքերի հայտնաբերում և վերլուծություն իրական ժամանակում,
   3. հաստատված միջադեպերին արձագանքում, որի ամբողջ գործընթացը պետք է կազմակերպված լինի միջազգային ստանդարտներին համապատասխան և ներառի հետևյալ փուլերը՝ նախապատրաստում (ուսուցում, հրահանգներ, մոնիթորինգ), հայտնաբերում, դասակարգում, արձագանքում, վերլուծություն, մշակում և հաշվետվություն, կանխարգելման միջոցառումներ (պարբերական աուդիտներ և թեստեր, համակարգերի արդիականացում և աշխատակիցների ուսուցում),
   4. Տեղեկատվական անվտանգության միջադեպերի ներքին հետաքնության համակարգ: Ցանկացած միջադեպ, որը որ տեղի է ունեցել կրիտիկական կոմպոնենտների հետ, և ազդել է ծառայությունների որակի վրա, պետք է անմիջապես տեղեկացվի Պատվիրատուին, և հակամիջոցների կիրառման մասին հաշվետվությունը (post-morterm report) պետք է տրամադրվի ոչ ուշ, քան հակազդող միջոցների կիրառումից հետո 48 ժամվա ընթացքում։
2. Կատարողն պետք է ապահովի 99,9% հասանելիության մակարդակ (համարժեք է տարեկան մոտավորապես 8 ժամ 45 րոպե անհասանելիության):
3. Տվյալների կենտրոնը պետք է կառավարվի շուրջօրյա (24/7 ռեժիմով)՝ պատրաստ արձագանքելու ցանկացած միջադեպի։
4. ՏՄԿ-ում պետք է առկա հուսալի ցանցային ենթակառուցվածք՝ պահուստային ցանցային սարքերով, ներառյալ՝ երթուղիչներ (routers), փոխարկիչներ (switches) և հրեպատեր (firewalls)։
5. ՏՄԿ-ի տեղանքը պետք է ընտրված լինի հաշվի առնելով և նվազեցնելով ջրհեղեղի, երկրաշարժի և շրջակա միջավայրի այլ գործոնների հնարավոր ազդեցությունը:
6. ՏՄԿ-ում պետք է առկա լինի Պատվիրատուի համար առանձնացված և վերջինիս պահանջներին համապատասխան թողունակության տրամադրման հնարավորություն:
7. ՏՄԿ-ում համակարգը պետք է նախագծված լինի այնպես, որ ինքնաշխատ կերպով հայտնաբերի անսարքությունները կամ խափանումներն առանձին բաղադրիչներում/մոդուլներում՝ կանխելով դրանց ծավալի մեծացումը և տարածումը համակարգի այլ մասերի վրա:
8. Կատարողը պետք է ունենա հետևյալ հավաստագիրը՝
   * ISO/IEC 27001 հավաստագիր
9. Կատարողն` իր կազմակերպչական, տեխնիկական և տեխնոլոգիական իր միջոցներով կամ երրորդ կողմի ներգրավմամբ, պետք է ապահովի Պատվիրատուի ցանկացած տեղեկատվության և դրանց կրիչների հետ աշխատանքը միջազգային ստանդարտներին (օրինակ՝ NIST 800-88 Guidelines for Media Sanitization) համապատասխան՝ սկսած տեղադրումից մինչև անվտանգ ոչնչացում։
10. Կատարողի ակտիվները կենտրոնացված կերպով պետք է կառավարվեն՝ համաձայն ISO/IEC ստանդարտի:

**Ծառայությունների մատուցում**

Կատարողը պետք է՝

1. Պորտալում տրամադրի օգտագործողի միջերես՝ ռեսուրսների ուղղակի կառավարման համար՝ առանց մատակարարի միջամտության,
2. Տրամադրի հաշիվների (օգտագործողի հաշիվներ/ամպային հաշիվներ/համակարգի հաշիվներ) ստեղծման և կառավարման կառուցվածքային և ստանդարտացված եղանակ, ինչպես նաև հնարավորություն՝ դիտելու, հետևելու և մշտադիտարկելու բոլոր ռեսուրսները (տվյալներ, ծառայություններ, ենթակառուցվածք), դրանց սպառումը,
3. Թույլատրի օգտագործողներին ստեղծել լրացուցիչ օգտատերեր և նրանց տրամադրել հասանելիություն ռեսուրսներին: Տվյալ հնարավորությունը նույնպես պետք է հասանելի լինի՝ օգտագործողի միջերեսի միջոցով,
4. Ապահովի առանց սահմանափակումների հասանելություն օգտագործողի միջերեսին՝ 99,9% հասանելիության մակարդակով (համարժեք է տարեկան մոտավորապես 8 ժամ 45 րոպե անհասանելիության),
5. Պատվիրատուին տրամադրի լիարժեք վերահսկողություն իր անվտանգության քաղաքականության նկատմամբ, ներառյալ՝ տվյալների և համակարգերի գաղտնիության, ամբողջականության և հասանելիության սահմանումը,
6. Ապահովի օգտատերերի հասանելիության քաղաքականության սահմանման, կիրառման և կառավարման հնարավորություն,
7. Ապահովի օգտատերերի՝ համապատասխան թույլտվություններով անհատական ​​հաշիվներ և անհատական հաշիվների խմբեր սահմանելու հնարավորություն,
8. Համաձայն ISO 27001 և ISO 27002 ստանդարտներում նկարագրված հասանելիությունների վերահսկում բաժնի՝ նվազագույնի հասցնի իր անձնակազմի ձեռքով հասանելիությունը դեպի հաշվողական հոսթեր (compute hosts, storage servers): Հաշվողական հոսթերի կառավարման գործողությունների մեծամասնությունը պետք է իրականացվի ինքնաշխատ (automated scripts) եղանակով։ Ձեռքով կատարված և ինքնաշխատ գործողությունները պետք է լոգավորվեն և պահպանվենտեղեկամատյաններում (logs) առնվազն 90 օր,
9. Պաշտպանի իր կողմից տրամադրվող ծառայությունները հրեպատներով,
10. Ապահովի Պատվիրատուի կողմից որոշ հրեպատային ծառայությունների կառավարում, ինչպիսիք են՝ GEO-IP ֆիլտրի կիրառման հնարավորություն, օգտագործողի կողմից կարգավորվող VPN ծառայություն և այլ գործառույթներ (համաձայն Պատվիրատուի պահանջի),
11. Ապահովի OSI 3-7 մակարդակներում ցանցային տրաֆիկի ամբողջական կառավարման գործիքակազմ՝ պատվիրատուի տվյալների հոսքի ամբողջ ճանապարհին,
12. Ապահովի արտաքին հարձակումներին հակազդող միջոցներ՝ OWASP Top 10 (վերջին ինկորպորացիայի) պահանջներին համապատասխան,
13. Ապահովի DDOS հարձակումներին հակազդող միջոց,
14. Տրամադրի տվյալների գաղտնագրման հնարավորություն՝ տվյալների պահեստներում և շտեմարաններում,
15. Տրամադրի գաղտնագրման բանալիների կառավարման ծառայություն, և որը հնարավորություն կտա Պատվիրատուին Կատարողի բանալիների կառավարման համակարգում ավելացնել, ստեղծել, վերահսկել և ջնջել իր սեփական գաղտնագրման բանալիները,
16. Տրամադրի մուտքի բանալիների (access keys) օգտագործման մասին տեղեկատվություն ստանալու, հին բանալիները փոխարինելու և ոչ ակտիվ բանալիները հեռացնելու հնարավորություն,
17. Ապահովի գաղտնագրման բանալիների երկարաժամկետ պաշտպանությունը՝ կանխարգելելով դրանց կորուստը կամ չարտոնված փոփոխությունները սարքավորումների խափանումների, ծրագրային ապահովման սխալների, տվյալների կենտրոնի խափանումների կամ այլ խափանումների դեպքում,
18. Ապահովի գաղտնագրման բանալիների կառավարման ճկուն տարբերակներ՝ որոնք թույլ կտան Պատվիրատուին ընտրել՝ արդյո՞ք Կատարողն է կառավարում գաղտնագրման բանալիները, թե՞ Պատվիրատուն է ստանձնում ամբողջական վերահսկողությունը,
19. Ապահովի Պատվիրատուի կողմից տվյալների լիակատար վերահսկողությունը, ինչպես նաև դրանց պահպանումը պետք է իրականացվի Պատվիրատուի հետ նախապես համաձայնեցված աշխարհագրական վայրերում (հասցեներում),
20. Ըստ պահանջի տրամադրի Real Static IP/subnet,
21. Թույլատրի Պատվիրատուին օգտագործել սեփական IP հասցեները՝ դինամիկ երթուղիների պրոտոկոլների (BGP, EIGRP, OSPF, etc.) միջոցով,
22. Իրականացնի տվյալների պահուստային տարբերակների կանոնակարգի (backup policy) և ժամանակացույցի (schedule) մշակումը և կառավարումն՝ ըստ պահանջի,
23. Ապահովի ռեսուրսների օգտագործման համար իրականացված վճարները՝ հաշվետվությունների և արտապատկերումների միջոցով՝ իրական ժամանակում տեսնելու և վերահսկելու մեխանիզմ։ Կատարողը նաև պետք է տրամադրի տվյալ ամսվա ռեսուրսների օգտագործման քանակի և վճարումների մասին տեղեկատվություն (համաձայնեցված ժամկետներում)՝ ինչպես մանրամասն, այնպես էլ ամփոփ տարբերակներով,
24. Ապահովի օգտագործված ռեսուրսների քանակի և ծախսերի օրինաչափությունների արտապատկերման, ինչպես նաև ապագա ծախսերի կանխատեսման մեխանիզմ,
25. Տրամադրի ռեսուրսների ամսեկան, եռամսյակային և ըստ օգտատերերի կամ օգտատերերի խմբերի սպառման շեմերի սահմանման և այդ շեմերը հատելու ծանուցումների ուղարկման ճկուն գործիքակազմ, օրինակ՝ ծանուցումների ուղարկում էլեկտրոնային փոստով կամ օգտագործողի միջերեսի միջոցով։ Գործիքակազմը պետք է ապահովի նախընտրած շեմեր սահմանելու և դրանք հեշտությամբ փոփոխելու ֆունկցիոնալություն։ Շեմերը պետք է լինեն ինչպես համամասնային (% of grand total), այնպես էլ հստակ արժեքներով (value),
26. Ապահովի ծառայությունների կատարողականի վերաբերյալ տեղեկատվություն՝ սույն հավելվածում ներկայացված պահանջների հետ համեմատական վերլուծության հիման վրա, հաշվետվությունների և արտապատկերումների միջոցով։

**Դեպի Կատարողի միջավայր միգրացիայի պահանջներ**

1. Կատարողը պետք է ապահովի Պատվիրատուի տեղային կամ այլ մատակարարների միջավայրերից ծառայությունների միգրացիայի գործիքակազմը, որը ներառում է սերվերներ, տվյալների շտեմարաններ, հավելվածներ և այլ ծառայություններ՝ ըստ Պատվիրատուի պահանջի:
2. Կատարողը չի սահմանափակում միգրացիայի ենթակա համակարգերի տեսակները։ Տարբեր վիրտուալիացիոն հարթակների (օր․՝ VMware կամ դրա համարժեք՝ HyperV .) միգրացիայի պահանջի առկայության դեպքում Պատվիրատուն  նախապես տեղեկացնում է Կատարողին էլեկտրոնային փոստի միջոցով՝ նշելով  միգրացիայի ենթակա համակարգի անունը և այլ անհրաժեշտ տեղեկատվություն։
3. Լայնամասշտաբ միգրացիայի դեպքում Կատարողը պետք է ապահովի միգրացիայի ավտոմատացման հնարավորություն, որն ապահովում է կրկնվող և կայուն (consistent) միգրացիոն գործողությունների իրականացում:
4. Հաշվի առնելով միգրացիայի աղբյուր և նպատակակետ հանդիսացող հարթակների (source/destination platforms) և միգրացիայի գործիքների պաշտոնական համատեղելիության փաստաթղթերը Կատարող պետք է ապահովի հետմիգրացիոն գործիքներ՝ հաստատելու տվյալների ճշգրտությունը, ամբողջականությունը և համատեղելիությունը:
5. Պատվիրատուի կողմից հին (Legacy) համակարգերի միգրացիայի պահանջի առկայության դեպքում՝ հաշվի առնելով միգրացիայի աղբյուր և նպատակակետ հանդիսացող հարթակների (source/destination platforms) և միգրացիայի գործիքների պաշտոնական համատեղելիության փաստաթղթերը Կատարողը պետք է իրականացնի խորհրդատվություն և առաջարկի համապատասխան լուծումներ, որոնք ապահովում են հին համակարգերի աշխատունակությունն և համատեղելիությունն Կատարողի միջավայրում:
6. Կատարողը պետք է ապահովի ռեսուրսների մինչև 200% մասշտաբայնացման հնարավորություն՝ ըստ Պատվիրատուի պահանջի, լայնածավալ միգրացիայի ընթացքում ծանրաբեռնվածությունը կարգավորելու նպատակով (ժամկետները հավելյալ համաձայնեցվում է մատակարարի հետ):
7. Կատարողը պետք է ապահովի միգրացիայի աջակցության ծառայություններ, ներառյալ՝ մասնագիտական ​​ուղղորդում և խորհրդատվություն՝ անվճար հիմունքներով, ինչպես նաև անհրաժեշտության դեպքում տեխնիկական օժանդակություն:
8. Տվյալների շտեմարանի պլանավորված միգրացիայի ընթացքում Կատարողը պետք է ապահովի իր կողմից տրամադրվող ծառայությունների 99,9% հասանելիության մակարդակ (համարժեք է տարեկան մոտավորապես 8 ժամ 45 րոպե անհասանելիության)։
9. Կատարողը պետք է ապահովի կենտրոնացված ծառայություն, որը թույլ կտա Պատվիրատուին իրական ժամանակում վերահսկել սերվերների և հավելվածների միգրացիայի կարգավիճակը և կատարողականը (օրինակ՝ սխալների քանակ, ուղղումներ և այլն):
10. Կատարողը պետք է տրամադրի միգրացիայի կարգավիճակի, համապատասխան չափորոշիչների և միգրացիայի պատմության արտապատկերման գործիքակազմ:

**Կատարողի միջավայրից ելքի ծրագրի (exit plan) պահանջներ**

1. Կատարողը պետք է տրամադրի իր միջավայրից դեպի Պատվիրատուի տեղային կամ այլ մատակարարի միջավայր տեղափոխվելու գործիքակազմ, ելքի ծրագիր (exit plan) և ծառայություններ, առանց Կատարողի միջավայրում արգելափակման (vendor lock-in):
2. Կատարողը պետք է ապահովի տվյալների տեղափոխման թափանցիկ և ստանդարտացված ընթացակարգ՝ ապահովելով գործիքակազմի, API-ների և գործընթացների հստակությունը:
3. Կատարողը պետք է տրամադրի միգրացիայի աջակցության անհատականացված ծառայություններ, ներառյալ՝ տեխնիկական և խորհրդատվական աջակցություն՝ Պատվիրատուի տվյալների տեղափոխման հատուկ կարիքների համար:
4. Կատարողը պետք է ապահովի տվյալների սահուն միգրացիան,
5. Պատվիրատուի տեղային կամ այլ մատակարարի միջավայր տեղափոխվելու դեպքում Կատարողը չպետք է ներկայացնի ավելորդ վճարների պահանջ, քան նախատեսված է պայմանագրի դրույթներով կամ այլ սահմանափակումներ:
6. Կատարողը պետք է ապահովի տվյալների արտահանումը Պատվիրատուի կողմից սահմանված ձևաչափերին և պրոտոկոլներին համապատասխան:
7. Կատարողը պետք է ապահովի կենտրոնացված ծառայություն, որի միջոցով Պատվիրատուն կարող է իրական ժամանակում վերահսկել իր սերվերների և հավելվածների միգրացիայի կարգավիճակը և կատարողականը (օրինակ՝ սխալների քանակ, ուղղումներ և այլն):
8. Միգրացիայի ավարտից հետո Կատարողը պետք է ապահովի Պատվիրատուի բոլոր տվյալների անվտանգ ջնջումը` և անհրաժեշտության դեպքում, պետք է տրամադրի ապացույցներ (օրինակ՝ ոչնչացման ակտ):

**Բիզնես անընդհատության, աղետների դիմակայման և վերականգման ծրագրեր**

1. Կատարողը պարտավոր է ունենալ Բիզնես անընդհատության և աղետների դիմակայման ծրագիր (այսուհետ՝ Ծրագիր)։
2. Կատարողը պետք է ունենա բնական աղետների արձագանքման և դրանց ազդեցությունը նվազեցնելու գործիքակազմ։
3. Տարին առնվազն մեկ անգամ Կատարողը պետք է իրականացնի բիզնես անընդհատության և աղետների դիմակայման և վերականգնման ծրագիր՝ Պատվիրատուին ներկայացնելով ամփոփ հաշվետվություն Ծրագրի արդյունքների մասին։

Ծրագրում պետքն է ներառված լինի համաճարակներին արձագանքման ընթացակարգ: Հնարավոր ազդեցությունների մեղմացման ռազմավարությունը կարող է ներառել տարբեր աշխարհագրական դիրքերում պահեստային թիմերի առկայությունը՝ հիմնաքարային գործընթացները տարածաշրջանից դուրս գտնվող թիմերին փոխանցելու համար: Հեռավար աշխատող անձնակազմի ցանկը նախապես տրամադրվում և հաստատվում է Պատվիրատուի կողմից։

**Լրացուցիչ պահանջներ**

* Հաշվողական, տվյալների պահպանման և ցանցային բոլոր ծառայություններն ապահովող սարքավորումները ծառայության մատուցման ամբողջ ընթացքում պետք է ֆիզիկապես գտնվեն Հայաստանի Հանրապետության տարածքում։
* Տեխնիկական պլանային աշխատանքների իրականացման անհրաժեշտության դեպքում նախապես համաձայնեցնել աշխատանքների կատարման օրը և ժամային ինտերվալը պատվիրատուի հետ, ոչ ուշ քան հինգ աշխատանքային օր:
* Ծառայությունները պետք է հասանելի լինեն առնվազն 99,9%-ով տարեկան։
* ՏՄԿ նկատմամբ միջազգային ստանդարտների համապատասխանության մասին բոլոր պահանջների մասով Պայմանագրի կատարման փուլում պետք է ներկայացնել համապատասխան պահանջը բավարարող կամ դրան համարժեք լուծումը հավաստող փաստաթուղթ (հավաստագիր), համապատասխան ոլորտը կարգավորող կամ ճանաչված, միջազգային համբավ ունեցող կառույցի կողմից։