#### **DRP for Remote Access Systems**

**Scenario:** VPN Server Failure  
**Objective:** Restore VPN services to ensure secure remote access for employees.

**Preparation**

* **Inventory:** Maintain an updated inventory of all VPN servers, configurations, and critical software versions.
* **Backups:** Regularly backup VPN configurations and critical system data to a secure, offsite location.
* **Documentation:** Ensure detailed documentation of VPN configurations, network topologies, and recovery procedures.

**Immediate Actions**

* **Detection and Alert:**
  + Monitor VPN server health with automated tools.
  + Set up alert systems to notify the IT team immediately upon detecting failure.
* **Initial Assessment:**
  + Determine the scope of the failure (hardware, software, configuration issue).
  + Check for common issues such as power failures, connectivity issues, or software crashes.

**Recovery Steps**

* **Step 1: Switch to Backup VPN Server**
  + Activate the pre-configured backup VPN server if available.
  + Update DNS records and inform employees about the switch.
* **Step 2: Troubleshoot Primary VPN Server**
  + If backup is not available or operational, start troubleshooting the primary VPN server.
  + Check server logs for errors and perform necessary repairs (e.g., restart services, replace hardware components).
* **Step 3: Reconfigure VPN Settings**
  + If configuration corruption is detected, restore the latest configuration from backups.
  + Verify security settings and user access controls.

**Post-Recovery**

* **Verification:**
  + Test the VPN connection from multiple locations and devices to ensure functionality.
  + Ensure that all users can access the network securely.
* **Communication:**
  + Inform employees about the restored service and any new access instructions.
  + Provide support for any connectivity issues they may face.
* **Documentation and Review:**
  + Document the incident, actions taken, and lessons learned.
  + Review and update the DRP based on the incident analysis.

### **DRP for Cloud Services**

**Scenario:** Cloud Service Provider Outage

**Objective:** Ensure business continuity by switching to an alternate provider or local backup systems.

**Step 1: Incident Identification and Notification**

* IT and cloud management teams are alerted to the outage.

**Step 2: Incident Assessment**

* Provider Status Check: Confirm the outage by checking the cloud provider's status page and communications.
* Verify the scope and impact of the outage

**Step 3: Activate Backup and Redundant Systems**

* Switch to Backup: switch to backup cloud providers or on-premises systems to restore critical services.

**Step 4: Temporary Workarounds**

* Alternative Solutions: use VPNs to connect to alternate data centers or leverage local servers.

**Step 5: Comprehensive Testing**

* Security Testing**:** Perform security checks to ensure that the integrity and security of cloud services are intact post-outage.

**Step 6: Post-Incident Review and Documentation**

* Update DRP**:** Revise the disaster recovery plan based on the lessons learned from the incident to improve future response.

**Step 7: Preventive Measures**

* Routine Inspections**:** Schedule regular maintenance and health checks for cloud services.