**Summary of Requirements**

**ITB-SEC-706340-2024**

 **For Provision of Disaster Recovery Services**

**Objective**
The Organization for Security and Co-operation in Europe (OSCE) seeks to procure a Disaster Recovery (DR) service for the re-establishment of critical IT infrastructure and systems following any natural, technological, or human-induced disasters. The DR service focuses on IT systems and excludes broader business continuity planning. The current DR system, implemented in 2014 at the OSCE Secretariat Data Center (DC) in Vienna, requires expansion and modernization.

**Scope of Services**

1. **Data Center Requirements**
	* The Disaster Recovery facility must be located within 50 km of Vienna.
	* The Data Center must be a Tier 3+ facility with ISO 27001 certification for security.
	* The Bidder may provide the services directly or via a data center from a local neutral carrier.
2. **Infrastructure Provision**
	* The vendor must provide server infrastructure to support 105 synchronized virtual machines (VMs) with 1788 GB memory and 390 vCores. There should be 10% spare capacity for future VMs, with five VMs running continuously.
	* The infrastructure must support additional physical devices, including 10-15 bare metal servers, a tape library, a KVM switch, and three network switches.
3. **Storage and Network Requirements**
	* The vendor must offer a storage system with self-encrypting drives, compatible with the current OSCE replication system, with an initial capacity of 100 TB and fast-class disk performance.
	* Redundant uplinks (1/10 GBit TP RJ45) must be provided, connecting to OSCE-owned switches.
4. **Administrative Access and Security**
	* OSCE must have full administrative access to all virtual infrastructure components.
	* The vendor must guarantee that OSCE data is never copied, replicated, or moved outside the dedicated DR environment without written consent.
	* Compliance with OSCE privacy rules is mandatory.

**Support and Maintenance**

* **Licenses and Subscriptions:** The vendor must provide and maintain all required virtualization software licenses and apply regular patches to the DR infrastructure.
* **Annual DR Tests:** The vendor must support OSCE in conducting annual DR tests, providing six desktops/notebooks for use during the tests.
* **Monitoring and Reporting:** Regular reporting on system status and patching is required, and changes affecting the DR infrastructure must be communicated two weeks in advance.
* **24/7 Support:** The vendor must offer a 24/7 English-speaking hotline for registered OSCE staff.

**Service Level Objectives**
The Disaster Recovery solution must support Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) of 24 to 48 hours, depending on the specific service.

**Conclusion**
The vendor must deliver a secure, compliant, and reliable DR service to safeguard OSCE's IT infrastructure, ensuring quick recovery and minimal disruption during disasters. The solution must be flexible, scalable, and fully compatible with OSCE's existing systems.