بسم الله الرحمن الرحيم

National Center for Security
& Crises Management

المركز الوطني للأمن وإدارة الأزمات

## اعلان استدراج عروض اسعار للشراء رقم م وأز/ادارة/ل/IT/٢٣/٢٠٢٤/ع٣٧

### شراء نظام إدارة صلاحيات الاتصال PAM

١. يعلن المركز الوطني للامن وادارة الازمات عن حاجته لشراء نظام إدارة صلاحيات الاتصال PAM وحسب المتطلبات المبينة بالملحق (أ) المرفق، فعلى الراغبين بتقديم عرض سعر معفي من الضريبة العامة على المبيعات ورسوم الاستيراد وأية رسوم وضرائب أخرى علماً بأن مشتريات المركز خاضعة بنسبة الصفر استنادا لنص المادة (٢٢/أ) من قانون الضريبة العامة على المبيعات موافاتنا بعروض فنية منفصل عن العرض المالية بالمغلف المختوم في المركز الوطني للامن وادارة الازمات/سكرتير لجنة الشراء الرئيسية (خلف متحف السيارات الملكي) على ان يكون العرض معزز بالسجل التجاري ورخص المهن مبيناً الرقم الوطني للشركة جميعها سارية المفعول.

٢. آخر موعد لتسليم المناقصات الى لجنة الشراء الرئيسية / سكرتير اللجنة يوم (الاثنين) الساعة (١٢٠٠) الموافق ٢٠٢٤/١٢/١٦.

٣. تطبق احكام وتعليمات نظام المشتريات الحكومية رقم (٨) لسنة ٢٠٢٢.

٤. لتسليم المناقصات التنسيق مع سكرتير لجنة الشراء الرئيسية على الرقم المباشر (٠٦٥٧٧٧٨٧٠) أو (٠٦٥٧٧٧٣٧٠) فرعي (٣٢٠٧) أو خلوي (٠٧٩٢١٢٢٢٦٨).

هاتف رقم (٠٦٥٧٧٧٣٧٠+) - (٠٦٥٧٧٧٤٦٠+) - (٠٦٥٥٥٠٠٥٥٥+) فرعي (٣٢٦١) فاكس (٠٦٥٤١٢٧٨٩+) www.ncscm.gov.jo
صندوق بريد ٨٥٥٠٣٣ الرمز البريدي ١١٨٥٥ - عمان - الأردن بريد إلكتروني dewan@ncscm.gov.jo

الملحق (أ) المتطلبات لشراء نظام إدارة صلاحيات الاتصال PAM للشراء
رقم م وأز/ادارة/ل/IT/ ٢٣/٢٠٢٤/ع٣٧

# National Center for Security and Crisis Management

## Request for proposal (RFP)

## Privileged Access Management (PAM)

# Technical RFP

## 1. Introduction:

The National Center for Security and Crises Management (NCSCM) is requesting proposals for the supply of Privileged Access Management (PAM) technology. NCSCM seeks an authorized resellers who are integrators that can provide product installation and professional services.

## 2. Scope of Work:

The selected vendor will be responsible for providing a robust, scalable, and secure Privileged Access Management (PAM) solution that meets the following requirements:

- Manage and secure privileged credentials for 10 administrators "privileged accounts".
- Support integration with existing systems.
- Ensure high availability and scalability for potential growth.
- Meet regulatory and compliance requirements relevant to the industry.

## 3. Terms and Conditions:

A) The bidder must have a proven track record of implementing PAM solutions for clients of similar size and industry.

B) Bidders must be an authorized partner for the proposed system; documents from the vendor to prove the partnership must be delivered within the technical proposal.

C) Demonstrate the technical capability of the team who will be in charge of maintaining and supporting the Privileged Access Management (PAM), by providing the team qualifications and the number of people who will support and maintain the SLA.

D) Bidder shall provide basic project management services for the implementation, and non-scheduled visits for all emergency cases upon NCSCM request.

E) A comprehensive site survey need to be conducted to ensure the successful deployment of the Privileged Access Management (PAM) solution.

F) The winning bidder shall provide 24/7/365 support services for Hardware (physical server), software, professional services and warranty.

## 4. Technical Specifications/Requirements :

### A- Credential Management

1. **Automated Credential Rotation:** Automatically rotate credentials (passwords, keys, tokens) based on predefined schedules or after usage.
2. **Password Complexity Enforcement:** Ensure compliance with organizational password policies.
3. **Integration with Secrets Management:** Support for development tools for securely managing secrets in CI/CD pipelines.
4. **SSH Key Management:** Centralized management, rotation, and logging of SSH keys.
5. **API Key Protection:** Secure storage and management of API keys for cloud and third-party services.

### B- Access Control

6. **Just-in-Time (JIT) Access:** Provide time-limited access to privileged accounts, reducing exposure.
7. **Granular Role-Based Access Control (RBAC):** Define access policies at a fine-grained level (e.g., user, team, department).
8. **Adaptive Authentication:** Enforce multifactor authentication (MFA) based on user behavior, location, and risk profiles.
9. **Workflow Approvals:** Require manager or admin approval for access to sensitive systems.

### C- Monitoring and Auditing

10. **Session Recording and Playback:** Record privileged sessions with the ability to search, audit, and replay for compliance purposes.
11. **Live Session Monitoring:** Allow real-time monitoring of active sessions to detect anomalies or unauthorized actions.
12. **Behavioral Analytics:** Use machine learning to detect unusual behavior patterns (e.g., unusual access times, high-risk commands).
13. **Comprehensive Audit Trails:** Log all activities performed by privileged users for accountability.
14. **SIEM Integration:** Export logs and alerts to Security Information and Event Management (SIEM) systems for centralized analysis.

### D- Integration Capabilities

15. **Directory Services:** Native support for Active Directory (AD), LDAP, and other directory services.
16. **Identity Governance Integration:** Align with Identity and Access Management (IAM) solutions to enhance compliance.