



MERCY CORPS

Request for Proposal **HQ357 Privilege Access Management System (PAMS)**

Date_09/02/2023_____

CONTENTS

I.	3
II.	3
III.	4
IV.	6
V.	6
VI.	7
VII. Sample Contract	6

I. Mercy Corps Overview

Mercy Corps is a global team of humanitarians, working together on the front lines of today's biggest crises to create a future of possibility, where everyone can prosper.

Our mission: to alleviate suffering, poverty and oppression by helping people build secure, productive and just communities.

In more than 40 countries around the world, our nearly 6,000 team members work side by side with people living through poverty, disaster, violent conflict and the acute impacts of climate change. We're committed to creating global change through local impact — 86 percent of our team members are from the countries where they work.

We bring a comprehensive approach to every challenge, addressing problems from multiple angles. Thanks to support from our extended global community, we've provided \$4 billion in lifesaving assistance to meet the urgent needs of more than 220 million people over nearly 40 years. In addition to emergency aid, we partner with local governments, forward-thinking corporations, social entrepreneurs and people living in fragile communities to develop bold solutions that make lasting change possible.

Through our impact, influence and innovations, in 2020 we:

- Reached nearly 38 million people in more than 40 countries.
- Raised \$60.5 million for our COVID-19 Resilience Fund and have reached 15.1 million people so far through our response.
- Provided 1.8 million people with emergency cash assistance.
- Our work in the Democratic Republic of the Congo alone reached more than 4.9 million people
- Secured \$490 million in revenue from institutional and private funders in 2019.
- Piloted the use of 3D printing to support children with disabilities in Jordan's Za'atari refugee camp.
- Sponsored the Global Fragility Act, together with a coalition of 70 grassroots organizations, which created the first-ever U.S. government strategy to tackle alarming levels of global violence around the world. The act was signed into law in December 2019 after receiving bipartisan support in Congress.
- Launched FInX with a \$10M contribution from Ripple and Rippleworks with the goal to accelerate global financial inclusion by advancing innovative, responsible distributed ledgers, digital assets, cryptocurrencies and other digital financial solutions that help people join the global economy and lift themselves out of poverty.

See more details about our impact in 2023: <http://www.mercycorps.org>

II. Project Background and Context

Background:

The cost of cyber-insurance for Mercy Corps (MC) has increased over the last three years, and last year many of our applications were rejected by insurance providers. Unrestricted local administrative rights were specifically noted as a reason for this rejection. Continuing use of this practice has made it difficult and expensive to obtain cyber-insurance.

For the purposes of this statement of work, the term “Project” means the acquisition, implementation, and establishment of initial maintenance procedures for a Privilege Access Management (PAM) system to mitigate the associated risks.

Mercy Corp is seeking for a proposed solution and professional services provider to support with the implementation of a Privilege Access Management System.

Purpose / Project Description:

The project will seek to remove these elevated rights, yet still allow users to perform necessary tasks safely on their computers, by using a Privilege Access Management (PAM) system. The PAM system will help protect against cyberthreats by exerting control over and monitoring the elevated (“privileged”) access and permissions for users, accounts, processes, and systems across an IT environment. The PAM system will control, monitor and act on the user’s behalf to perform high security tasks such as software installation.

Once implemented, a PAM administrator will use the PAM portal to define methods to access the privileged accounts across various applications and enterprise resources. The credentials of privileged accounts (such as their passwords) will be stored in a special-purpose and highly secure password vault that is deeply integrated into the PAM system. The PAM administrator will use the PAM portal to define the policies of who can assume access to these privileged accounts and under what conditions. Privileged users will log in through the PAM and request privileged access, or immediately assume access to the privilege’s user account, depending on context and case. This access will be logged and remain temporary for the exclusive performance of specific tasks. To ensure security, the PAM user should be asked to provide a business justification for using the account. The user shouldn’t be granted access to the actual passwords used to log into the applications but instead be provided access via the PAM. Additionally, the PAM will ensure that passwords frequently change, ideally automatically, either at regular intervals or after each use. The PAM administrator should be able to monitor user activities through the PAM portal and even manage live sessions in real time, if needed.

Initial rollout will include about 7,000 users, with an expected annual growth rate of about 5%.

III. Desired Services & Scope of Work

Objectives:

The objective of the Project is to acquire, implement, and establish the maintenance of a Privilege Access Management (PAM) system that meets the minimum requirements as established in the Project Charter.

Deliverables:

- Preparation of PAM implementation plan based on chosen vendor’s solution and identification of current system gaps.

Vendor / Solution Requirements:

- The PAM System must be able to standardize all endpoint users to a set of configurable, minimal, standard privileges.
 - This should include restrictions on software installation, usage, and OS configuration changes.
 - This should include the ability to allow users to add printers and other peripheral devices.
- The PAM System must automatically manage the routine privilege escalations of users who require privileged access to carry out specific tasks or use specific applications.
- The user should be able to inject credentials directly with the PAM System.
 - The user should never have to manually type administrative credentials.

- The PAM System should be able to supply this functionality without displaying the privileged credentials to the user.
- The PAM System should allow an endpoint user to submit a reason / business case when requesting non-routine temporary elevated access.
- The PAM system must tie into our existing SSO (Single-Sign On) technologies (Okta) and not require a separate log-in.
 - If the PAM system must become the initial log-in due to its design, it must allow Team Members to use MFA (Multi Factor Authentication).
- The end-user user interface must be intuitive and easy to use to best facilitate user adoption and mitigate workaround attempts.
- Passwords and secrets (passwords) on the local workstation should be rotated. Rotation should be able to be automatic, scheduled, and based on use.
- Password policies should be enforced by the PAM system, as it handles the rotation of the passwords, and governs aspects of passwords such as complexity, uniqueness, expiration, and the elimination of default passwords.
- Passwords must be securely stored and encrypted in a tamper-resistant safe/vault.
- The PAM System should passively track and analyze user behavior by collecting, storing, and indexing application use, session recordings, and other privileged events.
- The PAM System should be able to terminate or suspend any privileged account sessions that are deemed to be suspicious either automatically or upon review.
 - If a privileged account session is deemed suspicious, the PAM system should enable a rapid orchestration of security responses to stop or mitigate the detected threats.
- The PAM System must be able to be centrally administered / managed for policies, passwords, sessions, reporting, auditing, etc.
- The access control provided by the PAM System must be granular.
 - There is a need to be able to target groups and users.
 - There should be an ability to allow exceptions to existing policies.
- The PAM System must provide the ability to implement trust-based application whitelisting, with the flexibility to set both broad and granular rules.
- The PAM System must not require any additional third-party tools or potentially dangerous dependencies and should instead utilize native tools (example: MSTSC, PuTTY) and standard protocols for connections (example: RDP, HTTP/S, SSH, SAML, RADIUS) instead.
- The PAM System should include the ability to push agent updates to endpoints.
- The PAM System should be able to manage credentials across various platforms.
 - This must include Windows and Mac devices.
 - This must include cloud and web application credentials.
 - This would ideally include network and other devices such as Firewalls.
- The PAM System should allow flexible deployment options.
 - Hardware appliances
 - Virtual appliances
 - Software.
- The deployment should be agent-based and be able to be included in a system image for an image-based deployment to endpoints.
- Strong Reporting Capabilities
 - How privileged credentials are being used.
 - Privileged session activity.
- Strong Auditing Capabilities.
 - Track any changes to critical policy, system, application, and data files.
 - Unauthorized action attempts including detected workarounds.
- The PAM System cannot rely exclusively on, or even primarily, Active Directory alone. Mercy Corps does not utilize on-premises Active Directory.

Timeframe / Schedule:

- Work plan to be proposed.
- Anticipated start date February 2023 but open for discussion. Contract term is three months from the date of entering into an agreement.

IV. Evaluation of Proposals

Proposals will be scored using the following technical criteria. Points for each question will range from 0- 25 the maximum technical score is 100 points. Proposals should address each evaluation criteria.

- Adherence to the RFP Requirements: Did the bidder conform to all requirements and product or service specifications in the RFQ or RFP? (0-25)
- Technical Criteria: Includes the bidder's understanding of the service or procurement required, bidders' management plan, supplier's qualifications and bidders' overall resources. Does the supplier have the right qualifications (registration, insurance, experience)? (0-25)
- Management Criteria: Includes the bidder's experience on similar projects, bidder's performance on similar projects, bidder's available facilities and resources for the project and the bidder's plan for management and control of the project. (0-25)
- Cost Criteria: Is the cost within any pre-determined price range, such as cost estimates from a market analysis? In most cases cost is evaluated using value for money unless otherwise directed by donor requirements. (0-25)

An evaluation will be done by checking responsiveness to our requirements (proposals) and a follow up interview for a demo from the shortlisted bidders.

V. Proposal Format & Requirements

In order to secure information in a form, which will ensure that your proposal will be properly evaluated, you are asked to submit your proposal in the format listed below. Standard proposal formats are acceptable provided the following information is included:

1. Name, address, telephone number and email address for principal contact.
2. A brief outline of your organization and services offered, including:
 - Full legal name, jurisdiction of organization or incorporation and address of the company
 - Full legal name and country of citizenry of company's President and/or Chief Executive Officer, and all other officers and senior managers of the company
 - Year business was established
3. Name and professional qualifications of personnel who would provide the services.
4. Names, addresses, phone numbers and email addresses of at least two clients of similar industry and scope of operations as Mercy Corps that can be contacted as references.

CONTACT FOR BID INQUIRIES

All inquiries concerning this solicitation shall be addressed to the following Designated Contacts:

- **Gabriel Suarez**, Global Procurement Manager / gsuarez@mercycorps.org

Please email an electronic version of your response (via e-mail), including all supporting documentation, and direct questions about the RFP to each of the designated contacts.

All questions should be submitted in writing (via email) citing the particular bid section and paragraph number. Bidders should note that all clarifications and exceptions are to be resolved prior to the submission of a bid.

Only questions received during the Question and Answer period (as outlined in the RFP Calendar) will be addressed. No telephone questions will be answered. Official answers to the questions will be posted on Mercy Corps website at www.mercycorps.org/tenders

RFP CALENDAR/TIMELINE

- RFP published 13 February 2023
- Questions and Answers period 14 February 2023 to 27 February 2023
- RFP responses due 03 March 2023.
- Vendor e-meetings week of 06 March 2023.
- Vendor selected and notified ASAP

VI. Other Terms & Conditions

WITHDRAWAL OF RFP

Proposals may be withdrawn before the RFP submittal deadline by submitting a written request to the Contact Person. Re-submittal before the RFP submittal deadline can be made; however, they may not be re-submitted after the deadline.

RFP COSTS

All costs incurred in the preparation and presentation of proposals to the RFP shall be completely absorbed by the responding party to the RFP. All documents submitted as part of the RFP will become property of the Mercy Corps. Requests for specific material to be returned will be considered. Any material submitted that is confidential must be clearly marked as such.

AWARD BASIS

At the option of the Mercy Corps, finalists for the Agent designation may be selected for a final round of negotiations; however, applicants are encouraged to present their best offers with their initial submission. Mercy Corps reserves the right to accept or reject any and all proposals, to waive any irregularities in any proposal process, and to make an award of contract in any manner in which Mercy Corps, acting in the sole and exclusive exercise of its discretion, deems to be in Mercy Corps best interest.

CONTRACTUAL DEVELOPMENT

Once an applicant is approved as the exclusive Agent, the successful respondent will enter into a contract with the Mercy Corps. Contract discussion and negotiation will follow the award selection. Bidders must be amenable to inclusion, in a contract, of any information provided whether herein or in response to this RFP, or developed subsequently during the selection process.

CONTRACT TERMS

Firms that are selected as the exclusive Agent are eligible to enter into a service contract. Mercy Corps may terminate the contract upon written notice to the Agent of not less than thirty (30) days.

EQUAL OPPORTUNITY

Mercy Corps emphasizes that all respondents will receive full consideration without regard to race, color, religion, sex, national origin, sex, disability, age or sexual orientation. Minority and women-owned firms are especially encouraged to respond to this RFP.

LIMITATIONS

Mercy Corps, reserves the right to reject any and all Proposals and to waive any informality in the solicitation process. Total proposal length excluding cover letter, details of professionals who will provide services, and contact information of client references, should not exceed 12 pages.

VII. Sample Contract

The Sample Contract will be found in **Annex 2** is the anticipated contract and is a condition to the tender. However, if required, additional terms and conditions may be added by Mercy Corps in the final contract.

Any deviations or justifications from this contract must be set out in the tender proposal with proposed alternative language.