INVITATION TO REQUEST FOR PROPOSAL (RFP)

Identity Management and Governance tool

Norwegian **Red Cross**

Table of Contents

1. Introduction

Norwegian Red Cross invites your company (Respondent) to submit a response to this Request for Proposal (RFP). The final choice of the Vendor (One of the competing Respondents) shall be made on the basis of this process.

The Vendor is encouraged to use its NGO pricing models available for organisations such as the Norwegian Red Cross.

The purpose of this RFP process is to receive proposals and the possible sourcing of an **"Identity Management and governance tool"** from the market that will allow Norwegian Red Cross to source a platform that will handle day-to-day management of identities and their governance along with an implementation project.

The RFP therefore covers the expected features and charges of such an identity tool and associated implementation/support services.

2. About the Norwegian Red Cross

The Red Cross in Norway is a national association of the world's largest humanitarian aid organization; the International Red Cross and Red Crescent Movement. The organization is located in 190 countries and has around the world approximately 100 million members and volunteers. The basic idea of the Red Cross is to prevent and alleviate human suffering, both in local communities and in international conflicts.

Currently, the Red Cross in Norway has about 130,000 members and 50,000 volunteers divided into different activities. The Red Cross is organized with headquarters in Oslo, with 19 district offices and over 400 local offices around the country. The number of employees is in excess of 500 on a national basis.

See also www.rodekors.no.

3. Goals and Objectives

The IAM strategy workshops within Norwegian Red Cross have identified the following goals and objectives. The objectives outline the reason for the RFP process and the subsequent need for the sourcing of an Identity Management and Governance tool.

The implementation of the IAM strategy allows the Norwegian Red Cross:

- **Control of identities and their access**
    - Have ongoing control over the identities and accesses for employees, volunteers, delegates, members and external consultants
    - Ongoing re-conciliation and check of master data from two data sources for internal and external users

    - The ability to prove compliance to defined rules, regulations and policies
    - All roles and users get access to services based on their areas of responsibility and role definitions
    - Continuous and regular check of access based on roles
    - Continuous and regular check of licenses assigned based on roles
- **Support future delivery models**
    - Support for the increased use of cloud, hybrid delivery models and multiple vendor ecosystems
    - Flexible and speedy change management that supports an agile organisation

4. Criteria for selection of Vendor(s)

When selecting the Vendor, the following criteria will be considered (not in any specific order of priority):

- Product functionality and user-friendliness
- Integrations and out of box APIs available
- Price and payment model
- Availability and quality
- Service and support including implementation, consulting and training
- Vendor Competence/references
- Vendor Financial health/Credit rating

The Norwegian Red Cross will invite relevant Respondents to give a more detailed presentation and review of their proposals at a later stage in the process.

5. Scope of RFP

This RFP's scope covers several areas within the IAM ecosystem. The RFP covers both employees, delegates and volunteers working with the Norwegian Red Cross as set out in Section 9 of this RFP.

The Norwegian Red Cross has several situations where users have both internal and external roles (with access to applications and portals). The Respondent is requested to come up with solutions that cover an Enterprise Identity tool and an external Customer IAM for defined roles. Please note that this does not cover the donors for specific fundraising programs.

The following scope and features within Identity Management tool to be included in this RFP:

- Integrated workflow and automation
- Identity Definition through Customer attributes
- Identity Governance
- Delegated Administration
- Rules Engines

- Password Management
- Single sign-on integrations
- Role Engineering and Management
- Automated and manual Entitlements Management
- Self-Service applications
- Identity Federation
- Auditing & Reporting - Audit trail & Activity logging
- Data Integration and Synchronization
- Identity Management System Connectors
- Automated Configuration and administration
- Automated policy-based Revoke and/or De-registration
- Status monitoring, tracking and event notification
- Security policy enforcement through roles and entitlements
- Reduction in per user number of credentials

6. Detailed Functional Requirements

The list below is indicative set of features that are expected within the Identity Management tool. The Vendor shall within its response document clearly outline Yes/No in terms of compliance of its product to the below requirements.

6.1 User and Role management

- Support for user role definition and assignment of internal and external access rights based on roles
- Support User access and privileges from various platforms and applications
- Supports Cross-Internet-domain authentication and delegated authorization supporting industry standards such as SAML, OAuth, and OpenID.
- APIs with market login/authentication solutions e.g. OpenID, social logins, others for external users
- Support for commit and rollback of propagated changes (transaction-based synchronization)
- Support for database-maintained change log for event triggered updates
- Support for identity mapping from a person object to one or more account objects based on security requests from identity administrators
- Supports Role Mining to discover potential roles
- Directly configured Role types
- Supports hierarchical role models with n levels
- Ability to import roles using manual or automated interfaces
- Analysis of roles based on usage, control, membership, access and risk profile
- Reports on all users and privileges within a type of account or role or group
- Supports temporary assignment of access or roles to a user with revoke dates and dates
- Out of the box Risk based model approach to roles and accounts
- Support recording of provisioning activities for Audit purposes

- Provides easy user registration services that include:
    - Feeds from authorized source systems
    - Self-user registration request with workflow process
- Templates can be configured to effect changes to all users or groups created based upon template
- Template-based workflows for user account creation, management, group assignments, de-activation and deletion
- Solution supports the creation of a one-time password for a new user and indicate the methods to communicate that password to the user
- Automated creation, pending workflow approval(s) of user and group accounts based on attribute information
- Prohibits requests that would not be approved based upon predefined conflicts, attributes, role, or some other facet of the requestor
- Supports multiple workflow request initiation from a user or an administrator

6.2 Roles Management

- Product analyses and reports existing privileges to identify possible Roles
- Performs Role attestation
- Delegation capabilities exist within Product Role engine
- Interface for managing Roles
- Entitlements used to make the roles actionable in Product interface
- Support user-initiated requests for new roles and entitlements through the workflow engine
- Identity Contracts are maintained in product and what alerts are available at each stage of the contract lifecycle
- Support for Persistent and non-persistent user information
- Supports Trust based federation in identities

6.3 Password Management and SSO

- Support for self-service password reset
- Support for password push to selectable target systems (i.e., the user or administrator is allowed to specify which systems have the same passwords)
- Support for user-defined challenge-response questions and answers
- Support for pre-defined challenge-response questions and answers
- Support for configurable challenge-response rules (e.g., user will be allowed to reset password and IDM/target account will be unlocked after correctly answering three out of five; user account will be locked if more than two questions are answered incorrectly; etc.)
- Web-based GUI interface for password reset functions
- Support for IVR and/or telephony interface for resetting passwords
- Self-service password reset application may be presented as a portal/web GUI
- Delegated Administrators (e.g., End User Help Desk) can reset IDM/target password (create a new one-time password) without knowledge of current password
- Delegated Administrators (e.g., End User Help Desk, Cloud administrators) can escalate to 2nd level support (e.g., IT Security)

- Support for password change detection & synchronization from AD
- Support for top-down password push from IDM solution to database credential repositories (such as Microsoft SQL Server, and Oracle)
- Support for bulk password updates or resets based upon administrator-defined groups of users
- Support for password dictionary checking
- Support for password strength checking
- Support for password hints or suggestions
- Support for workstation lockout scenario
- Support denial of access protection by blocking repeated password failures on multiple administrator accounts in the directory
- Support for Single-Sign-On (SSO) integrations out of the box
- Support for multiple-factor authentication
- Support for self-service lost password recovery by creating a new onetime password based on successful answer(s) to pre-configured secret questions. This must also result in account unlocking for the user
- Support for identity administrator reset of user password for a one-time use on IDM/target account
- Support for identity administrator to unlock IDM/target user account after too many failures on IDM/target account

6.5 Administration and other features

- Product detects changes that need to be processed
- Schedule-based and event driven updates
- Merges and resolves differences between attribute values
- GUI-based run-time view of workflow status by identity administrator, by identity subject (e.g., the person being administered) or by overall system administrator
- Supports workflow routing to specific approval administrators (e.g., administrators, application owners, managers) based on Cost Centre, Group ownership or other specific attributes
- Allows for Approvers to authenticate to the identity management system to access the workflow inbox and perform the workflow activity
- Support for key browsers such as Internet Explorer, Edge, Chrome, Safari, Firefox etc.
- Supports Email notifications to specific accounts or groups of accounts for certain activities performed by the identity management system
- Workflow escalation based on configurable response time windows on a per workflow basis function
- Support for workflow, initiated by administrator or authorized user action
    - Event-driven activation or de-activation
    - Request-driven activation or de-activation
- Supports workflow for disabling and deletion of accounts in separate steps
- Supports removal of different type of customer accounts and user ID (person object) from identity management system upon deletion
- Support for the creation of platform-specific entities required for account provisioning
- Manual and automated delegation capabilities

- Web-based GUI delegated administration interface for workflow interaction
- Supports dynamic delegation to specific identity administrators based on a user's attribute values (cost centre, job code, etc.)
- Supports delegation by identity administrator to another person for a specific period of time
- Support for reminders to identity administrators who are required to perform workflow tasks
- Support for multiple level delegation
- Supports self-registration security requests for specific services
- Timestamp and auditable tracking of all actions
- Supports Customization of the Product interface/UI

6.6 Integrations and connectors

- Supports integrations to standard market applications, databases and directory services with bi-directional synchronization
- Detailed list of out of the box API's (App stores) and protocols that your workflow engine supports
- Prevents changes to data in connected systems so that information acquired from authoritative sources is maintained
- Support request for the creation of a new LDAP group through the identity management interface with workflow approval for group creation. Approval results in creation of new group object on identity manager (directory) and either LDAP security systems
- Support for pull-based and push-based synchronization (polling)
- Discovers attributes and objects that are not fully synchronized at any given moment and forces a resynchronization
- Toolkit for creation of connectors and APIs/Web interfaces
- Product can spawn multiple workflows from a single instruction or workflow
- Support auto generation of tickets through integration with ITSM systems
- Integration with Enterprise Mail such as O365 or Exchange Server
- Supports API integrations with other systems such as
    - HR systems
    - CRM systems
    - Marketing tools
    - Reporting tools
    - Customer service & support solutions
    - ITSM/Project tools
    - Cyber security tools
    - Tailored-COTS/COTS
    - SaaS based applications

6.7 Analytics, Auditing and Reporting

- Real-time and batch analysis (behaviour analysis)
- Monitoring & Reporting
    - Captures source, identity, group and endpoint attributes

  - Derived context from Applications
  - Current User Location tracking support
  - IP address-based actions - trusted, blacklisted, anonymous
  - Access characteristics
  - MAC addresses
- General Monitoring capability and automatic recovery options are available for both the Identity Management engine and any connectors
- Support out-of-the-box report views
- Supports scheduled report generation
- Supports email-based report subscriptions / notifications
- Supports a built-in query tool for ad-hoc reporting
- Supports configuration of security audit levels and audit information collected
- Support user maintenance auditing (identity updates, password changes, self-administration, etc.) Support for historical reporting
- Support for integration with other reporting engines such as Power BI etc.
- "Dashboard" interface that can be used to quickly identify important events and Role based dashboard reports
- Supports creation and distribution of customized reporting and dashboards
- Provides standard templates/workflow
- Supports High Availability, Disaster Recovery configurations
- Supports various environments such as Development, Test and Production including moving of any customization across the environments
- If on-premise, supports virtualized environment Setup (VMWare or Hyper-V)
- If SaaS, has upgrade roadmap with version upgrades included in subscription

7. Implementation of Product

The Respondent shall also outline the following within its proposal document:

- Respondents´ framework for implementation
- Suggested timeline for the implementation projects
- Reference Architecture for implementation
- Requirements from the Norwegian Red Cross (Resources and Documentation)
- Change Management and Training
- Phased onboarding of applications and requirements

8. Support and Maintenance

The Vendor shall provide the following support and maintenance for its product:

- Ongoing application maintenance and support training
- Warranty support for all software.
- A detailed Service Level Agreement (SLA) as agreed upon by both Norwegian Red Cross and the Vendor

- The Vendor shall provide all technical, operational, and administrative knowledge transfers required for Customer or its 3rd Party personnel to successfully conduct activities related to the deployed solution.
- Technical training materials and classes including both onsite and distance/online delivery.
- End-user training materials and classes including both onsite and distance/online delivery.

9. Volumes

The Norwegian Red Cross has several types of users/identities who will be impacted by the rollout of the Identity Management solution. The Vendor shall consider the following volumes for the pricing.

Departments within the Norwegian Red Cross (Employees):

- National and district/local offices
- International
- Fundraising
- Communication
- Human Resources
- Finance and Administration

There are four distinct types of users with several categories of sub-profiles.

In Scope

- Employees: 700 internal users
- Delegates: 300 internal users
- Volunteers: 45.000 external users
- Total number of systems/applications: 40-50 systems

Future Scope (Overlapping roles)

- Members: 150.000+ external users (not in scope, information only)
- Regular donors: 95000+ external users (not in scope, information only)

Given that the users could be in several combinations of profiles at any given point in time, the Norwegian Red Cross sees the need to identify unique roles/combinations and a chosen IAM system must be able to handle changes in these roles across the HR and CRM (Internal and External) solutions simultaneously.

9.1 Integrations and onboarding for first roll out

The following applications and integrations shall be considered within the scope to be onboarded for the first phase of rollout of the Identity Management system.

#	System name	Application type	Description	Type
1	Active Directory	Basic Services	On-premise AD	Integration
2	Azure AD	Basic Services	Azure AD	Integration
3	Visma HR	SaaS	HR system for internal user data expected to be operational from May 2019	Master data-source integration
4	MS Dynamics CRM	Tailored COTS	Dynamics CRM for external user data (on-premise)	Master data-source integration
5	MS Dynamics AX	Tailored COTS	Financial accounting system (on-premise)	Master data-source integration
6	Office 365	SaaS	End user computing solutions	Onboarding
7	Unit4/Agresso	Tailored COTS	Financial accounting system (on-premise)	Onboarding
8	Berg-Hansen portal	Portal	Travel portal	Onboarding/User registrations

10. Pricing

The Vendor is expected to submit a price based on the following volumes in the separate pricing sheet attached with this RFP document. The objective is to estimate the TCO for the Norwegian Red cross over a five-year period.

It may be noted that the Norwegian Red Cross has a preference for SaaS based solutions.

The Respondent may change the model with the same principles intact in order to reflect its price model.

On Premise solution

In the event that the Respondent is offering an On-premise version that meets all the requirements stated in the RFP, the Respondent is requested to fill out the pricing template for OP1 through to OP5 including the charges for its implementation partners.

SaaS solution

In the event that the Respondent is offering a full SaaS version that meets all the requirements stated in the RFP, the Respondent is requested to fill out the pricing template for SA1 through to SA3 including the charges for its implementation partners.

Optional charges

The Respondent shall outline additional optional charges that may be exercised by the Norwegian Red cross on its sole discretion.

11. RFP timeline and details

The response shall be delivered electronically through Mercell as per the defined structure. Vendor is requested to follow the documentation requirements stated within the following sections.

11.1 Timeline for RFP

The following dates shall be followed for the response to this RFP.

#	Activity	Format requirements	Final Date
1	Send out of this RFP	This PDF document	Week 51
2	Last date to submit questions to this RFP	Mercell Q&A portal	21. January 2018
3	Proposal from interested Vendors	Delivered as per Section 11.2	28. January 2019
4	Vendor Presentations	Vendor shall present its offer and technical proposal	Week 6 – Week 8
5	Shortlisting and selection of final Vendor	Norwegian Red Cross evaluates the proposals and presentations to make final selections. If needed, additional presentations may be scheduled to reach a conclusion.	February - March 2019
6	Contract negotiations and signing	Negotiation of final terms and conditions/signing of contract.	Q1 - Q2 2019
7	Planned implementation start date	Expected start timeline for implementation	Q2 2019

11.2 Response documentation requirements

Respondents shall deliver the following in their response with the following structure:

- **Cover letter** signed by a person authorised to commit Respondent to this RFP
- Vendors shall respond in a separate **Proposal Document (Vendors own format)** how the product meets the requirements and the implementation timeline. The product compliance requirements in **Section 6** shall be included within the Respondents proposal document.
- Vendors shall include their **Product documentation/standard terms and conditions** as a

part of their response

- **Price template** based on **(Section 10)**
- Any **Reservations and Assumptions** to the Response
- The following documentation must be enclosed in separate documents:
    - **Company name, registration, org. number and address**
    - **Company presentation**
    - Relevant **References (at least 3)** from similar implementations.
    - **CVs of planned resources for implementation**
    - **Security documents** (Cloud security, DR etc.)
    - **Credit rating/Financial Report** for the last three years
    - Other relevant documentation for subcontractors (if relevant)

11.3 Communication during the RFP phase

Questions to the request should be addressed via the communication module in Mercell. All incoming questions shall be anonymized, and responses shall be published to all participating Vendors in order to ensure equal treatment of all Respondents.

- The Norwegian Red Cross reserves the right to correct and supplement the request within the deadline.
- Notification of changes will be sent to Vendors who have notified an interest to respond to the RFP in Mercell.

11.4 Reservations and Assumptions

Any reservations and assumptions to any part or formulation stated within this request, must be specified in the offer to be valid. Reservations that cannot be calculated in terms of cost may result in the offer being considered incomplete and rejected.

11.5 Administrative Provisions to the RFP

The following administrative provisions shall apply for the RFP process:

- This document is only a request for information about potential products / services and does not hold the Norwegian Red Cross liable for any contractual obligations.
- Norwegian Red Cross reserves the right to negotiate further in relation to selected proposals.
- The Norwegian Red cross reserves the right to cancel all or parts of this competition at any point during this RFP.
- The Norwegian Red Cross reserves the right to reject proposals.
- Expenses incurred by Vendor in connection with the preparation of the proposals and the process leading up to a contract being signed will not be refunded
- Vendor may use subcontractors for its services. In such case, the Vendor shall be responsible for all tasks performed by the subcontractor. If the Vendor uses

subcontractors or partners, responsibility for the delivery will be a business matter between Vendor and its subcontractors, as will any legal, financial and other matters between the parties. The use of subcontractors shall not entail any increased costs for The Norwegian Red Cross. The company name and organisation number of any subcontractors must be stated.

- The Norwegian Red Cross will treat all information from Vendor confidentially. Vendor cannot make all or parts of the invitation to RFP public without The Norwegian Red Cross´s written permission.

11.6 Confidentiality

This invitation to RFP with enclosures is the property of the Norwegian Red Cross and must not be reproduced beyond what is necessary for internal consideration. The documents cannot be used or disclosed to a third party without the Norwegian Red Cross´s written consent. The parties undertake to maintain confidentiality in relation to the content of proposals and documents used in the competitive proposal procedure and information they may receive about each other and each other's business.

12. General Terms and Conditions

12.1 Contract term

The contract term shall be an initial period of Implementation + Monthly subscription costs for running costs. Respondent shall clearly outline the termination conditions and relevant effects for the Norwegian Red Cross.

12.2 Validity of the proposal

The proposal shall be valid for 6 months after the date the offer is delivered.

12.3 Pricing terms

The Norwegian Red Cross wishes to have predictable and fixed costs and hence the requirement for a monthly subscription cost. Vendor is encouraged to provide special pricing models for organisations such as the Norwegian Red Cross.

12.3.1 NGO Pricing model

It is noted that several Respondents state the availability of a special pricing models for NGOs such as the Norwegian Red Cross. Respondents shall provide these pricing structures as per the pricing format stated. Respondents may also submit alternative pricing models if relevant.

12.3.2 Invoicing Requirements

The Norwegian Red Cross has the following requirements to invoicing:

- Electronic invoicing through the format EHF (for Norway based Vendors)
- Invoices shall have a 30-day payment term from the date of receipt of the correct invoice
- Invoices shall be marked “everog” in the buyers reference field. No other fields shall be populated.