Project title: BPRA Zanzibar Business Registration System

Annex on Information Security

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH operates an Information Security Management System (ISMS) and is planning certification to ISO/IEC 27001, which will be maintained. Certification always documents implementation of the current version of this standard.

The following information security regulations apply to service delivery:

1 Right of audit

For the entire duration of the project term, the contractor shall grant GIZ the right to audit the security of the information processed by the contractor.

Unless audits are a response to a specific situation, they may generally be carried out no more than once per year. Before any such audit commences, GIZ shall inform the contractor (in good time) of the initial object and the planned scope of the audit, to enable the contractor to plan accordingly.

In the context of service delivery by the contractor, GIZ has the right to audit the service delivered, including the necessary associated infrastructural, organisational, personnel and technical components. This right of audit can also be exercised by third parties acting on behalf of GIZ.

The contractor shall not be recompensed separately for expenses incurred by supporting/performing GIZ's audits.

2 Minimum requirements for means of authentication/passwords

As a minimum, the contractor shall implement the following requirements for password quality for all accounts with which it accesses/can access GIZ information:

- Passwords shall be at least 10 characters long; passwords for privileged accounts shall be at least 16 characters long.
- Passwords for technical accounts shall be at least 20 characters long if passwords cannot be changed regularly (e.g. using Managed Service Accounts).
- A password shall contain three of these four character types: uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9) and special characters (for example !, $, #, %).
- Passwords that are easy to guess may not be used.
- The password must not contain all or part of your login name!
- A password may not be identical to one of the last 10 passwords used.
- Passwords shall be changed regularly, max. password age 90 days.
- after 10 wrong entries the account should be locked for 30 minutes

Multi-factor authentication (at least two factors) shall be used for accounts with administrative permissions.

3 User certificate errors

Measures shall be taken to ensure that certificate errors do not occur when certificates are used.

4 Minimum requirements for data backup

The contractor shall meet the following requirements for the procedure for backing up the processed data:

- The data backup must enable the complete restoration of the technical components/applications required for the service provided and all data in accordance with the following parameters:
  - Data backup shall take place at least once a week (RPO: seven days).
  - Restoration of all technical components/applications shall not take longer than 48 hours (RTO).
  - Data backups shall be retained for a minimum of 30 days.
- The technical components and the storage location for the data backup shall be sited in two different fire compartments.

5 Contractor's ISMS

The contractor shall have an appropriate, documented Information Security Management System (ISMS) installed, which satisfies the ISO/IEC 27001:2022 standard (or its latest subsequent version) or a similar standard. The ISMS shall cover the service to be delivered, including the information to be processed along with the necessary associated infrastructural, organisational, personnel and technical components.

The contractor shall appoint a chief information security officer who has the required expertise, and shall inform GIZ of his/her contact details upon request.

GIZ shall appoint an exclusive contact person to handle all the contractor's questions relating to information security.

6 User management

The contractor's ISMS shall include procedures for the documented award, change, locking, unlocking, deactivation and reactivation of (privileged, internal, external and other) user accounts for the unequivocal identification of authorised persons and for resetting passwords.

These procedures shall include technical measures to protect against brute-force attacks (e.g. locking user accounts after multiple failed attempts at authentication).

The contractor shall ensure that its ISMS implements the following aspects of user management:

- User IDs shall be deactivated if they are no longer needed, or if they will not be needed for more than six months.
- User IDs may be deleted only if the deletion does not entail the risk that existing protocols, log files or other records can no longer be unequivocally matched to a person within the archiving period.
- When non-personal user accounts (e.g. root account, user accounts for IT emergencies) are used, suitable measures shall be in place to ensure that the activities conducted using these accounts can be definitively matched at any time to a particular person taking action or a particular responsible person (automatically if possible).
- Technical user accounts may be used solely by services or scripts. These accounts should not be used by a person.
- Technical user accounts may be configured only with minimum permissions in accordance with the permission concept. The principle of least privilege shall be implemented.
- Privileged user accounts may be used solely for administrative activities.

- When privileged user accounts for external users are created, they shall be set to expire after a maximum period of six months, after which they can be extended if necessary.
- User accounts for external users may be issued for a limited period only, which may not exceed one year. The period shall be based on the term of the contract with the external user. Accounts can be actively renewed as necessary.

The contractor shall ensure that administrative activities are performed only through personal accounts and that these accounts are used solely for administrative purposes.

7 Permission management

The contractor's ISMS shall include a documented procedure for the documented approval, award, change, correction, regular updating and prompt withdrawal of permissions.

The contractor's permission concepts shall be based on the principles of 'need to know' and 'least privilege', and shall be implemented effectively.

In the context of permission management, the requirements for the segregation of duties shall be implemented.

The permission concept shall include technical and organisational measures that ensure the effectiveness of the permission concept.

8 Change and patch management

The contractor's ISMS shall include procedures for test, change and patch management based on common standards (e.g. ITIL), so that secure, regular implementation (at least once every six months), and immediate implementation in response to specific situations, of (security) patches and updates are guaranteed for the service delivered.

9 Segregation of the test and production environments

The contractor's ISMS and the technical measures shall ensure that vulnerabilities, user errors and technical faults in test environments do not pose a risk to the production environment (e.g. by using a firewall to separate the test environment from the production environment).

Test environments shall map all significant features of the respective production environments.

10 Management of security incidents

The process for recognising, prioritising, remedying and documenting security incidents and other disruptions shall include the central recording and evaluation of relevant log data.

11 Vulnerability management

The contractor shall implement a procedure for recognising, evaluating (e.g. CVSS), prioritising, eliminating and documenting vulnerabilities for the service delivered.

The contractor shall report to GIZ every quarter on the recognised vulnerabilities that are relevant to the service to be delivered, and on their evaluation and elimination.

The contractor shall implement a procedure for regular (at least once per year), automated and logged vulnerability scans.

12 Hardening concept

The contractor shall implement a procedure for hardening the technical components. In particular, the procedure shall ensure that:

- unnecessary or unwanted services and interfaces are deactivated,
- unnecessary user IDs are either deactivated or deleted,
- default passwords are changed.

13 Internal audits

The contractor shall implement a procedure which includes regular audits – and audits in response to specific situations – of security measures in order to assess their suitability and effectiveness (for example comparisons of the actual and target states of configurations, firewall rules and penetration tests), and which records the audit results.

After notification by GIZ, the contractor shall allow external penetration tests to be performed either by GIZ or by third parties (no more than once per year).

Deficits identified by internal audits or penetration tests shall be remedied by the contractor without delay. The remedial measures shall be carried out by the contractor without separate remuneration.

14 Administrators' workplaces

The contractor shall ensure that systems can be accessed for administrative purposes only from hardened, monitored workplaces with restricted access.

15 Protection against malware

The contractor shall implement a procedure for the uninterrupted protection of technical components against malware and a response concept for large-scale malware attacks (e.g. ransomware).

16 Data backup concept

The contractor shall implement a procedure for data backup, which includes regular and documented tests of the restoration of data backups.

17 Segregation of clients

The contractor shall implement a technical procedure for segregating clients, which ensures that the information and processing contexts of different clients are kept separate.

18 Managing means of authentication

The contractor shall implement a procedure to be used for securely changing, sending and receiving, saving and storing means of authentication (e.g. passwords), and a regulation governing secure management of the means of authentication (e.g. passwords).

Any misuse of means of authentication shall be regarded as a security incident and dealt with accordingly.

19 Erasure concept

The contractor shall implement a procedure for the return, the complete (i.e. not re-constructible) erasure and the destruction of data, so that data classified by GIZ as 'no longer needed' are erased without delay, provided that they are not subject to any statutory or contractual retention or waiting periods, and erasure is possible with reasonable technical effort.

This procedure shall be applied in particular to GIZ information upon the scheduled or unscheduled termination of service delivery.

Upon request, GIZ shall be provided with a declaration or other evidence of the erasure. Evidence of the erasure procedure shall be provided upon request.

20 Secure firewall operation

The contractor shall implement a suitable procedure which ensures that all firewalls are operated with minimum rules (whitelisting).

The rules shall be documented, and the current status of the firewalls' rule configuration shall be regularly compared with the documented target status.

21 Use of cryptography – cryptography concept

The contractor shall implement a procedure which includes the effective use of cryptography and key management to protect the confidentiality, authenticity and integrity of information.

During transmission and saving of GIZ data, the contractor shall ensure appropriate encryption (both in transit and at rest).

Communication via non-trustworthy connections (e.g. Wi-Fi, internet) in particular shall be appropriately encrypted.

The contractor's encryption protocols and procedures shall apply the latest technology.

22 IT emergency management

The contractor shall have an appropriate, documented IT emergency management installed which covers the service to be delivered, including the information to be processed along with the necessary associated infrastructural, organisational, personnel and technical components.

The contractor's IT emergency management shall be subject to a continuous improvement process.

As a minimum, the IT emergency management shall cover the following scenarios:

- failure of a building
- failure of a computer centre
- failure of the communication infrastructure.

Emergency tests for these scenarios shall be regularly performed and documented. The results of the emergency tests shall be used for making improvements.

23 Hosting

Virtual servers must be provided for the project.

Separation of application and data is to be provided, i.e. an application server and a separate server for the database and file storage is provided, with communication through a firewall.

All backups must be stored on a separate storage system set up specifically for this purpose.

A firewall must be installed upstream of every server and a up-to-date anti-virus software must be used on these servers and configured accordingly for automatic updates.

When configuring the web server, you must pay attention to the following:

- Disable Trace HTTP Request
- Run as a separate User & Group
- Disable signature
- Disable banner
- Restrict access to a specific network or IP
- Use only TLS 1.2

- Disable Directory Listing
- Remove unnecessary DSO modules
- Disable Null and Weak Ciphers
- periodically updates of the system -> stay current!
- periodically checks of the system log files

24 Software development

Separate environments for development, test and production must be provided.

The software to be developed and the development process shall satisfy the following requirements:

- Information security shall be the top priority for both the architecture and the functionality of the application ('security by design', 'information security through technology design').
- All IT systems and applications involved in software development shall be hardened in a suitable manner.
- Information about the framework used must not be included in the source code of the generated web pages.
- The application to be developed shall be operable with minimum system rights.
- Network communication between the components of the application should be encrypted.
- Transmission of authentication information (particularly passwords) shall be encrypted.
- The system must be hardened against SQL injection. In detail, this concerns the validation, filtering and cleansing of user input. The inputs may only have expected properties and characters and may not contain any unauthorized metacharacters that are passed to the SQL interpreter. When implementing API interfaces, it is essential to harden them against malicious code injection (SQL injection, etc.) via the URL.
- The system must be protected against Cross Site Scripting (XXS) on the client side. The server(s) must be protected against reflected or persistent cross site scripting by securing the server source code. All data to be processed by the server must be validated before execution. Whitelists of permitted data can be used for this purpose. General conversion of certain script characters is also a popular method. It is to be prevented that executable metacharacters of the scripts are read by the server. Cookies should only be read by the server (HttpOnly) and not by JavaScript in the browser.
- The application may not contain hard-coded passwords.
- The application should not contain hard-coded keys (symmetric/asymmetric). If this is unavoidable, a description of how to handle the key shall be available. The information security risks associated with storing the key shall be assessed.
- The application should be designed so that it can be tested and easily maintained (e.g. vulnerabilities can be remedied easily).
- Session cookies used for logins must be deleted after logging out from the client.
- To minimise incorrect use (human error), the application should be ergonomically designed to be secure and appropriate to the required level of protection.
- Entries made by users, data streams and secondary data (e.g. session information) shall always be validated, i.e. the application may not accept impermissible entries. Validation shall be performed in such a way that it cannot be circumvented (e.g. by manipulated client software).

- The error messages generated by the application (especially exceptions) may not provide any information that allows conclusions to be drawn about the architecture or the software/versions used.
- Users may not access application functionality or processed information until they have been authenticated/authorised.
- A documented permission concept is required for each application (e.g. in the operating manual).
- Chapter 2, "**Minimum Requirements for Authentication Methods/Passwords**," must be strictly observed
- Passwords may not be stored in plain text. Passwords may be stored only in hashed form. The hash algorithm shall apply the latest technology.
- For every application, a concept for recording logs shall be documented (e.g. in the operating manual), ensuring that the logs are recorded in a standard format. As a minimum, the following events shall be recorded:
  - successful and failed logins
  - changes to permissions and roles
  - user administration activities
  - other security-related events in the application.
- A role and authorization concept must be implemented that includes at least the roles of system admin (full authorization to the entire system), CMS admin (+account management), editor and author (editing content/articles). The application to be developed must be operable with minimal system rights. Only the following user groups may have access to the backend: Developers and administrators of the Contractor as well as employees for editorial maintenance of the Contractor.
- Access to the backend at the operating system level may therefore only be granted to very limited user groups with the appropriate expertise.
- There must be a documented authorization concept for each application (e.g. in the operating manual).
- For the upload of files, appropriate file filters are to be provided so that no files with executable content (scripts, programs or SQL codes) can be uploaded and executed.
- The deletion procedure must be proven upon request. Legal retention obligations remain unaffected.
- Confidential information and data may only be transmitted by email in encrypted form. If it is not possible to encrypt the email, this content must be packed into a ZiP archive which is secured by a complex password (see password policy). These passwords must be transmitted via a different communication channel.
- Only the SFTP protocol may be used for electronic file transfer, access must be secured with complex passwords (see password policy) and, if possible, 2FA/MFA should be used.
- Remote maintenance of systems may only be carried out via secure communication channels such as HTTPS with an encryption standard of at least TLS 1.2 or higher. So-called VPNs and SSH can also be used for remote support and maintenance, these must be configured/secured by a firewall at the endpoints.