1.1. Information Security Requirements

The below must be evidenced through official documentation. The bidder can submit a confirmation letter from the head of information security on a company letterhead to provide surety that the below information security controls have been implemented OR provide a reference/s to the organisations official publication which confirm that the following information security controls have been implemented.

Authentication and Access Control

1.1.1. The system must authenticate CSIR employees making use of CSIR's authentication authority.

1.1.2. The system must have user account management with the capability to assign and revoke different user roles.

1.1.3. The system must have the option to enable multi-factor authentication

1.1.4. The system must have the capability for session timeouts as a result of inactivity.

Data Security (Encryption and Privacy) & Privacy

1.1.5. The system's data allows for the latest (secured) encryption standard to be enabled when the data is stored.

1.1.6. The system's data allows for the latest (secured) encryption standard to be enabled when the data is in transit.

Risk and Vulnerability Management

1.1.7. The system's manufacturer must have conducted a vulnerability assessment (penetration test) on the solution.

1.1.8. The system's manufacturer must be able to provide security related support for the solution.

1.1.9. There is a secure implementation design that is recommended by the manufacturer.

1.1.10. Regular vulnerability scans are conducted on the system. Found vulnerabilities are managed.

Logs and Backups

1.1.11. The system logs capture important security event data.

1.1.12. Incident response support can be made available, should an information security related incident occur.