Procedure	Security Vulnerability Disclosure

1 Aim

Intercede are aware of the sensitive nature of the systems and networks our software is used to protect, and as such, take the security of Intercede solutions extremely seriously.

Intercede understand that from time-to-time security vulnerabilities in software may be discovered, and that people want to be able to report them directly to Intercede. These vulnerability reports are encouraged as they can provide valuable information that Intercede can use to improve the security of our software.

The aim of this policy is to define a clear security vulnerability reporting process, covering:

- How to report a vulnerability
- How Intercede deal with reported vulnerabilities
- How Intercede respond to reported vulnerabilities

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

2 Reporting

If you believe you have found a security vulnerability, please submit your report to us by emailing security.notifications@intercede.com

3 What to expect

After you have submitted your report, it will be assessed by an Intercede team including representatives from Product Management and the Office of the CTO.

Intercede aim to respond to your report within 5 working days and aim to triage your report within 10 working days. We also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Reporters should note that vulnerability reports may take some time to triage or address.

Intercede will notify you when a reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Intercede will take responsibility for disclosing vulnerabilities and remediation to our customers and partners in an appropriate and timely manner, therefore any reported security vulnerability should be treated as confidential between Intercede and the vulnerability reporter.

4 Guidance

When investigating or reporting a potential security vulnerability, individuals should consider the following guidance:

- Applicable laws and regulations must be followed, including data protection rules
- Reporter must not communicate any vulnerabilities or associated details other than by means described in the published security.txt file.

- Reporter must not demand financial compensation in order to disclose any vulnerabilities
- Any sensitive data related to the creation of a security vulnerability report must be deleted as soon as it is no longer required or within 1 month of a resolution for the vulnerability being provided, whichever occurs first (or as otherwise required by data protection law)
- This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give security vulnerability reporters permission to act in any manner that is inconsistent with applicable laws, or which might cause the organisation or partner organisations to be in breach of any legal obligations

5 Security.txt

Security.txt is an IETF Internet informational specification (RFC 9116) that describes a text file that webmasters can host that advertises the organisation's vulnerability disclosure process so that someone can quickly find all the information needed to report a vulnerability.

Intercede's security.txt file contains three key fields:
• CONTACT: email security.notifications@intercede.com or (https://www.intercede.com/vulnerability-disclosure/ detailing information required to be sent in the email)
• POLICY: link to Intercede's organisation's vulnerability disclosure policy.
• EXPIRES: Expiry date of security.txt file (one year from publishing)

6 Security Vulnerability Report format

The following data will be requested in any emails to security.notifications@intercede.com where applicable. Items marked as (M) are mandatory.
The purpose of the report is to capture the reporter's perceived information, the final assessment of weakness and severity will be based upon Intercede analysis.

Title (M)	Concise summary categorising the vulnerability
Product (M)	Name and version of the product affected
Weakness	Based on the Common Weakness Enumeration CWE
Severity	Such as low, medium, high or critical, calculated via the NIST Common Vulnerability Scoring System Calculator CVSS
Description of the Vulnerability (M)	A summary of the vulnerability Supporting files (e.g. screenshot or video) Any mitigations or recommendations
Steps to reproduce	Clear and descriptive steps to reproduce the vulnerability
Impact	The effect(s) of successfully exploiting the vulnerability.
Contact details	Name, Email Address, Organisation, Phone Number These details are optional to enable anonymous reporting

7 Security Vulnerability Response Report

Once assessed and as applicable, Intercede will provide the following information on a reported security vulnerability:

- Title: Concise summary categorising the vulnerability
- Product: Product and version where the vulnerability has been identified
- Weakness: based on the Common Weakness Enumeration system
- Severity: For example, low. Medium, high or critical, as defined by the NIST Common Vulnerability Scoring System Calculator
- Description: A summary of the vulnerability
- Impact: The effects of a successful vulnerability exploit
- Mitigation: information on how to address the vulnerability which may take the form of configuration or applying a software update