Appendix 1 – Escalation

Incident Response Management Handbook

Document Information

Version:	1.0
Datum:	12. 01. 2021
Status:	Final
Author:	Samuel Mühlebach, CISO Fides Treasury Services AG
Classification:	Intern

Content

1. Cyber Incident Escalation

The Appendix 1 of the incident response management handbook of Fides Treasury Services AG (FTS) documents the additional 3rd party escalation notes which need to be informed in case of a Cyber incident Level (CRISI or MAJOR).

2. FINMA reporting

2.1. Key statements:

- Communication to FINMA is done by CS Reg Affairs team
- Legal Entities with own IT infrastructure, to inform CS CISO and CS Reg Affairs team once they are aware of a cyber-attack potentially requires reporting to FINMA
- When relying on CS infrastructure, Legal Entity contacts will be included in the reporting process / task force

2.2. Action:

- Each Legal Entity to define their contact incl. deputy for FINMA reporting topic, see process documents chapter 11,
- In case the Legal Entity is reporting to FINMA at their own, access to EHP has to be ensured
- For Legal Entities which need to provide the information for reporting CS Reg Affairs, ensure you know the data source of 24h / 72h report
- Ensure relevant teams and Legal Entity management is aware of the FINMA requirement and the process.

2.3. Report:

- Reporting Procedure for FINMA Guidance 05-2020 Duty to report cyber attacks

3. SWIFT Customer Support

3.1. What

Contact the SWIFT Customer Support Centre and notify the support analyst of the security incident and the current status.

3.2. Prerequisites

The person in charge of this action must be registered on swift.com and have the role ‘Access to support via Case Manager, phone or e-mail’.

3.3. How

Support contact details are available on swift.com. Europe Tel: +31 71 582 2822

3.4. Who

The point of contact between you and SWIFT for the duration of the incident.

3.5. Why

SWIFT Support can help you to perform some of the actions defined in this document (e.g. identifying possible fraudulent messages by providing necessary data to perform proper business reconciliation).

SWIFT on behalf of itself and the entire SWIFT user community has a strong interest in keeping apprised of the circumstances surrounding any possible security incidents that can adversely affect customers’ use of SWIFT services and products. The contracts between SWIFT and its customers (including the customer organization) provide that in case of any problems relating to SWIFT services and products, the SWIFT user must notify SWIFT of the problem and assist SWIFT in identifying and investigating the problem. This covers particular incidents aimed at compromising the security of your SWIFT-related infrastructure or use of SWIFT services and products (see clause 13.2.2 of the Customer Security Programme - Terms and Conditions).

3.6. Documentation

Escalation\SWIFT Cyber Incident Recovery Roadmap.pdf

4. Zürich Financial Services

4.1. Dedicated Contact

Tatjana Mury
Finance, Investment & Treasury Portfolio - Compliance
Group Functions and Shared Utilities
IT Services, Group Operations

Zurich Insurance Company
Hagenholzstrasse 60
8050 Zurich
Switzerland

+41 (0) 44 628 19 86 (direct)
+41 (0) 79 252 21 18 (mobile)
+41 (0) 44 625 92 28 (fax)
tatjana.mury@zurich.com