PUBLIC
ÖFFENTLICH

APPENDIX 17-H
INFORMATION SECURITY
DUE DILLIGENCE, DUE CARE & ETHICS FOR PARTNERS AND SUPPLIERS

November 2024

Guidelines for the tendering party

This document contains specific information that MAN provides to tendering parties for the purpose of responding to requests for proposal.

Instructions for the tendering party

1. The tendering party undertakes not to amend or modify this document in any way.
2. The tendering party's response to this request for proposal should reflect the information contained in this document and correspond to this data.
3. Any objections or problems in connection with the definitions contained in the documents do not render the requirements set out in this document or in the request for proposal invalid, nor do they result in said requirements being modified. The tendering party can only assume that the changes it proposes are accepted if MAN has expressly confirmed this to the tendering party in writing.

Contents

SUMMARY

In today's business environment, forethought is mandatory. Hence, demonstrating due diligence and due care is the only way to disprove negligence in a possible occurrence of loss.

This Appendix outlines MAN's requirements towards ensuring sufficient availability and performance for the supply of products and services by taking current cyber security threats into account and responding adequately to those.

Further in the document an information is available about cyber incident reporting channels, main principles of conduct and awareness, as well as fair competition.

The information security due diligence obligations and the Information Security Code of Ethics are an integral part of the service contract.

It shall be ensured that all the partners or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners.

1. Due diligence and due care obligations for partners, service providers and suppliers

Since the provision and availability of critical services is permanently exposed to a wide range of threats, such as:

- Destruction of information by computer viruses
- Malicious encryption of critical data by ransomware attacks
- Theft of information via social engineering attacks – spying on passwords, phishing
- Loss or theft of data storage media or computers
- Failure of systems due to power outages, sabotage, vandalism, natural disasters

proactive measures to protect them must be implemented with urgency by MAN's partners, service providers and suppliers in order to ensure the contractually agreed service levels of availability and performance to MAN.

Protection will only be effective if it is based on a variety of interconnected measures and safeguards. The necessary minimum security measures to be implemented by partners, service providers and suppliers of MTB include among others, in particular:

- Effective protection of IT systems against external attacks through regular vulnerability analysis and timely security patch management
- Continuously raising security awareness among all employees, in particular social engineering attacks such as phishing as well as the channels to report events and incidents/see code of conduct B.
- Compliance internally with defined processes and procedures as well as externally with country and international laws, standards and regulations
- An appropriate and regular risk oriented reporting of the design and effectiveness of information security and operational processes - security related reports, compliance reports, threat analysis of the current landscape
- Appointment of an individual responsible for information security, particularly a function responsible for information security incidents and how to handle and report them to MAN and the respective authorities.

2. Information Security Code of Ethics

Corporate responsibility involves a duty to comply with all rules and regulations in force. Therefore MAN expects its suppliers and business partners to especially observe the basic principles that follow in this section.

This Information Security Code of Ethics sets out the benefit of ethical values to organisational behavior but also the expecations that MAN imposes to its suppliers and partners how they should behave in critical situations as well as the core principles that should guide their activities and decision-making.

The aims of the Code may be summarized as follows:

- Provide diligent measures to protect and ensure the contractually agreed service levels and performance
- Demonstrate responsibility and competence in the event of cyber attacks
- Repudiate any acts of corruption, bribary and unlawful or unethical behavior
- Ensure transparent business relationships and fair competition – refer to the MAN Code of Conduct for Suppliers
- Comply with MAN’s information security policies and guidelines, as listed in Annex 17 and Appendix 17-A
- Comply with legal requirements, regulations and standards

3. Duties for partner and suppliers

Ensure adequate level of awareness among employees and sub-contractors

Most attacks target the "human" factor as the supposed weakest link in the IT security chain.

Using false identities, cybercriminals try to mislead their victims into disclosing sensitive information, bypassing protective measures or installing malware on their systems themselves.

This increasingly happens in the form of so-called phishing e-mails, a sub-form of "social engineering". Both the phishing e-mail itself and the website to which a link in the text of the phishing e-mail refers look deceptively real by using logos, colours and fonts of the respective organisation or company that pretends to have sent the phishing e-mail to inspire confidence in the recipient. Often, the recipient is led to believe that there is an urgent need for action - for example, a current security incident or a credit card that has been blocked as a precaution. The phishing e-mails are often linked to current events.

Phishing e-mails pose a great danger not only when sensitive information is leaked, but also when malicious attachments are opened. A successful phishing attack is often the trigger for a subsequent ransomware attack. Data is encrypted to subsequently demand a ransom from the recipient of the phishing e-mail. Threats to delete or publish data are made if the ransom demand is not met in time. System destruction can also be the result of phishing emails or a ransomware attack.

With regard to the ever-increasing cyber security and threat situation, we ask you to be particularly alert and to sensitise your employees accordingly. We recommend that you take special care with e-mails from superiors that build up pressure or use a sharp tone. In case of doubt, such e-mails should be forwarded to appropriately trained personnel for further investigation. By recognizing a "social engineering" attempt rapidly, major damage can be prevented.

Report cyber incidents and behave adequately in the event of cybercrimes:

If you are affected by a cyber attack, please report the incident immediately to the to the MAN Truck & Bus Cyber Defense Center at mtb-cdc@man.eu

We recommend the following:

- Do not respond to demands for payment.

- Contact the central contact point for cybercrime at the state criminal police office responsible for your area
- Report the attack to the Federal Office for Information Security. There you will receive valuable information and advice on how to deal with the incident.
- File a criminal complaint with the police. Especially if your company is being black-mailed by using encryption Trojans.

Adhere to and implement basic security principles:

- Responsibilities: The roles and responsibilities of individuals involved with the contracted service must be clearly defined and match to the employee's competences and obligation.
- Separation of duties: The privileges to fulfill critical tasks must be separated appropriately among individuals in order to prevent the misuse of systems and undermining of processes.
- Least privilege: Users should only be provided with the minimum levels of access (or permissions) needed to peform their job function.
- Need to know: Users should only be provided with access to information and resources that are required to fulfill a task in line with their job function.
- Traceability: Important events must be recorded and analysed regularly in order to detect and fully investigate malicious activities