

Security Policy   
Incident Handling

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Incident Handling | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Group | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of contents

[1 Principle 4](#_Toc153531746)

[2 Objective 4](#_Toc153531747)

[3 Controls 4](#_Toc153531748)

[3.1 Identification of information security incidents 5](#_Toc153531749)

[3.2 Response to information security incidents 14](#_Toc153531750)

[3.3 Remediation of information security incidents 14](#_Toc153531751)

[3.4 Follow-up and reporting of information security incidents 15](#_Toc153531752)

# Principle

Information security incidents should be identified, handled, resolved and followed up using an information security incident management process.

# Objective

Quickly and effectively identify, resolve and report information security incidents, minimize the impact on the business and reduce the risk of similar incidents.

# Controls

A NIST SP 800-61 Rev. 2 compliant process for handling information security incidents must be in place that includes at least the following:

* Identification of information security incidents
  + Receiving reports on information security incidents,
  + Assessment of the business impact,
  + Categorization and classification of the information security incident and
  + Recording information about the information security incident
* Response to information security incidents
  + Escalation to the information security incident management team,
  + Investigation,
  + Containment and
  + Elimination of the cause of the information security incident)
* Resolving information security incidents (e.g. rebuilding systems and restoring data and closing the information security incident)
* Follow-up of information security incidents (e.g. post-incident activities such as root cause analysis, forensic investigation, reporting to the organization and notification of a security breach to the relevant authorities).
* Reporting serious security incidents to national authorities

The operational process for handling security incidents must comply with the requirements of the following NIST-800-61 Rev. 2 compliant business processes:

|  |  |
| --- | --- |
| "Identify and Record": | "Respond: |
| "Recover and Close: | "Follow up": |

## Identification of information security incidents

Information security incidents must:

* can be identified, e.g.
  + IT helpdesk processes,
  + Analysis of suspicious or unusual activities reported by business users,
  + the evaluation of information from security incident management tools
  + Information provided by a Security Operations Center
  + by notifying external parties (e.g. CERTs or law enforcement authorities)
* recorded in a log or equivalent document (e.g. with an automated security incident management system)
* categorized (e.g. according to severity and type). The categorization and classification of an incident must take into account at least the following aspects, which must also be documented as a whole:
  + The number and/or relevance of clients or other financial counterparties affected by the incident and, where applicable, the value or number of transactions affected and whether the incident has caused reputational damage;
  + Duration of the incident, including service downtime;
  + geographical spread of the SÜDVERS companies and SÜDVERS locations affected by the incident
  + the loss of availability, authenticity, integrity or confidentiality of data associated with the incident;
  + Criticality of the services concerned, including the transactions and business of the financial company;
  + economic impact for SÜDVERS - in particular direct and indirect costs and losses - of the incident on an absolute and relative basis
* The following scheme must be applied:

Ein Bild, das Text, Screenshot, Diagramm, Rechteck enthält.

Automatisch generierte Beschreibung

The following criteria must be applied:

Ein Bild, das Text, Screenshot, Zahl, Software enthält.

Automatisch generierte Beschreibung

For information security incidents that fulfill at least one criterion for a major incident in accordance with the DORA Regulation, at least the following information must be recorded:

| Number | Description |
| --- | --- |
| 2.1 | Date and time of detection of the incident |
| 2.2 | Date and time of classification of the incident as major |
| 2.3 | Description of the incident  Financial entities shall provide a high-level overview of the following information such as possible causes, immediate impacts, systems affected, and others. In subsequent reports, the field content can evolve over time to reflect the ongoing understanding of the ICT-related incident.  Description of any other relevant information about the incident not captured by the data fields, including the internal severity assessment by the financial entity.  For recurring incidents, financial entities shall provide information about each recurring incident, including date and time of its occurrence. |
| 2.4 | Classification criteria that triggered the incident report |
| 2.5 | Materiality thresholds for the classification criterion 'Geographical spread' |
| 2.6 | Discovery of the incident |
| 2.7 | Indication whether the incident originates from a third party provider or another financial entity |
| 2.8 | Impact or potential impact on other financial entities and/or third-party providers |
| 2.9 | Description of how other financial entities have been affected by the incident, where known, or reasonably expected. The description should include the following information about the other financial entities, if known:  1. name/group/activity/region,  2. entity type(s),  3. description of disruption incurred,  4. relationship (counterparty/service recipient/service provider). |
| 2.10 | Description of how third-party providers have been affected by the incident where known, or reasonably expected. The description should include the following information about the third-party provider(s), if known:  1. name/group/activity/region,  2. service provided and their type,  3. criticality of service,  4. description of disruption incurred,  5. location of incident source if known |
| 2.11 | Information whether the major incident has been recurring |
| 2.12 | Number of occurrences of the same incident |
| 2.13 | Information on whether the incident relates to a previous incident |
| 2.14 | Date and time of activation of business continuity plan, if activated |
| 2.15 | Information on activated business continuity plan:  The description shall include:   * the plan element(s) activated (e.g. full DR, specific recovery playbook, crisis communications) * date and time of activation of this measure * the extent to which this activation has addressed or is expected to address the incident <full recovery in x hours, par-tial recovery of critical services in y hours with |
|  |  |
| 3.3 | Date and time of occurrence of the incident |
| 3.4 | Date and time of occurrence of recurring incidents |
| 3.5 | Date and time when services, activities and/or operations have been restored |
| 3.6 | Number of clients affected by the ICT-related incident, which may be natural or legal persons, that make use of the service provided by the financial entity |
| 3.7 | Percentage of clients affected by the ICT-related incident in relation to the total number of clients that make use of the affected service provided by the financial entity. In case of more than one service affected, these shall be provided in an aggregated manner. |
| 3.8 | Number of financial counterparts affected |
| 3.9 | Percentage of financial counterparts affected |
| 3.10 | Impact on relevant clients or financial counterpart |
| 3.11 | Number of affected transactions |
| 3.12 | Percentage of affected transactions in relation to the regular level of domestic and cross-border transactions carried out by the financial entity related to the affected service |
| 3.13 | Total value of the transactions affected by the ICT-related incident |
| 3.14 | Information whether the numbers are actual or estimates |
| 3.15 | Reputational impact |
| 3.16 | Contextual information about the reputational impact  Information describing how the ICT-related incident has affected or could affect the reputation of the financial entity, such as infringements of law, regulatory requirements not met, number of client complaints and others.  The contextual information may include additional information, such as type of media (e.g. traditional, social media, blogs, social networks, streaming platforms) and media coverage, including reach of the media (local, national, international). It should be noted that media coverage in this context does not mean only a few negative comments by followers or users of social networks.  The financial entity shall also indicate whether the media coverage highlighted significant risks for its clients in relation to the incident, such as the risk of the financial entity's insolvency or the risk of losing funds.  Financial entities shall also indicate whether it has provided information to the media that served to reliably inform the public about the incident and its consequences.  Financial entities may also indicate whether there was false information in the media in relation to the incident, including information based on deliberate misinformation spread by threat actors, or information relating to or illustrating defacement of the financial entity's website.  Field mandatory to be reported with the intermediate and final reports if 'Reputational impact' criterion met. |
| 3.17 | The duration of the ICT-related incident shall be measured from the moment the incident occurs until the moment when the incident is resolved |
| 3.18 | Service downtime measured from the moment the service(s)is fully or partially unavailable to clients and/or financial counterparts to the moment when regular activities/operations have been restored to the level of service(s) that was provided prior to the incident. Where multiple services are impacted, the service downtime should measure until all services are restored. |
| 3.19 | Information whether the numbers for duration and service downtime are actual or estimates. |
| 3.20 | Types of impact in the Member States |
| 3.21 | Description of how the incident has an impact in other Member States |
| 3.22 | Type of data losses that the ICT-related incident entails in relation to availability, authenticity, integrity and confidentiality of data. |
| 3.23 | Description of the impact of the incident on availability, authenticity, integrity and confidentiality of critical data |
| 3.24 | Materiality thresholds for the classification criterion 'Critical services affected' |
| 3.25 | Comments to the classification criteria |
| 3.26 | Type of the incident |
| 3.27 | Threats and techniques used by the threat actor  The following threats and techniques shall be considered:   * Social engineering, including phishing * (D)DoS * Data encryption for impact, including ransomware * Resource hijacking * Data exfiltration and manipulation, including identity theft * Data destruction * Defacement * Supply-chain attack * Other (please specify) |
| 3.28 | Other types of techniques |
| 3.29 | Information about affected functional areas and business processes  The functional areas may include but are not limited to:   * Marketing and business * Customer * Product * Regulatory * Risk * Finance and * HR and general * Information Technology * Business   The business processes may include but are not limited to:   * Account * Actuarial * Acquiring of payment * Authority/client on-boarding * Benefit * Benefit payment * Buying and selling packages insurances policies between insurances * Card * Cash * Cash placement and/or withdrawals * Claim * Claim process * Clearing * Corporate loans * Collective * Credit * Custody and asset * Customer * Data * Data * Direct * Export * Finalizing trades/deals trade floors * Financial instruments * Fund * FX * Investment * Investment * Issuing of payment * Lending * Life insurance payments * Money * Net asset * Order * Payment * Policy underwriting * Portfolio * Premium * Settlement * Transaction |
| 3.30 | Information on whether infrastructure components (servers, operating systems, software, application servers, middleware, network components, others) supporting business processes have been affected by the incident. |
| 3.31 | Information about affected infrastructure components supporting business processes |
| 3.32 | Information on whether financial entity has communicated to the clients and/or financial counterparts about the incident and about the measures that have been taken to mitigate the adverse effects |
| 3.33 | Information about communication to clients/financial counterparts  The description shall include items such as the scope of the information contained in the communication, the means of communication with clients and/or financial counterparts, where possible, the categories of recipients and if communication was required under the financial entity's communication strategy.  Mandatory to be reported with the intermediate report only if the financial entity has communicated with its clients and/or financial counterparts. |
| 3.34 | Reporting to other authorities |
| 3.35 | Specification of 'other' authorities |
| 3.36 | Temporary actions/measures taken or planned to be taken to recover from the incident |
| 3.37 | Description of any temporary actions and measures taken or planned to be taken to recover from the incident  The information shall include description of the immediate actions taken such as isolation of the incident at the network level, workaround procedures activated, USB ports blocked, Disaster Recovery site activated, any other additional security controls temporarily put in place.  Financial entities shall also indicate the date and the time of the implementation of the temporary actions and the expected date of return to the primary site. For any temporary actions that have not been implemented but are still planned, indication of the date by when their implementation is foreseen.  If no temporary actions/measures have been taken, please indicate the reason.  Data field mandatory for the intermediate report if temporary actions/measures have been taken or are planned to be taken |
| 3.38 | Information on involvement of CSIRTs in dealing with the incident.  This description should include an indication of the nature of the CSIRT's involvement in handling the incident with reference to the following CSIRT incident management services.  The 'Incident Report Acceptance' category covers the CSIRT's receipt, triage and processing of an initial notification or subsequent incident reports. It concerns the support of the CSIRT in the initial phase of incident handling.  The 'Incident Analysis' category includes CSIRT support in the following areas: incident prioritization and categorization, information gathering, detailed analysis coordination, root cause analysis or cross-incident correlation. The 'Artifact and Forensic Evidence Analysis' category includes CSIRT involvement in media or surface analysis, reverse engineering, runtime or dynamic analysis, or comparative analysis. Both categories include the CSIRT's involvement in clarifying the causes and course of the incident and its impact on the financial entity in the next phase of incident handling.  The 'Mitigation and Recovery' category may be reported by the financial entity if the CSIRT was involved in ad hoc response and containment, system restoration or other mitigation and recovery support.  If the CSIRT has been involved in activities related to the coordination of incident handling, the financial entity should indicate on 'Incident Coordination' category. This includes support from the CSIRT related to:   * communication, * notification distribution, * relevant information distribution, * activities coordination, * reporting or * media communication.   If the CSIRT provided support in the area of crisis management, the category 'Crisis Management Support' should be indicated. |
| 3.40 | Information related to the incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable. |
| 3.41 | Description of the vulnerabilities exploited during the incident, including weaknesses, susceptibility or flaw of ICT products or ICT services.  Description of the vulnerabilities exploited during the incident, including weaknesses, susceptibility or flaw of ICT products or ICT services.  The description should include an indication of whether any vulnerabilities have been exploited in connection with the incident and, if so, to provide the relevant information, including, but not limited to:   * Information about the affected products, their versions, configurations, patches and extensions * Information about the affected platforms and operating systems (including their configuration) * Information about the manufacturer or provider of the vulnerable ICT products or ICT services * Description of the vulnerability, including information about the exploitation of the vulnerability - for unpublished vulnerabilities * Own assessment of criticality: low/medium/high/critical - for unpublished * Applied mitigation measures (workarounds or hot fixes)   Information about the manufacturer or provider of the vulnerable ICT products or ICT services may include, in particular, the name or other data identifying the ICT third-party service provider. If the provider is not also the manufacturer of the ICT product affected by the vulnerability, it is also important to provide information that allows identification of the manufacturer of such a product.  When providing information on how the vulnerability was exploited, the effects/impacts of the vulnerability may be considered in the first place.  The description should also include the assessment of the criticality of the vulnerability by using common industry standards.  The description should also include whether other authorities have been notified of the vulnerability and whether the provider/manufacturer has been contacted. |
|  |  |
| 4.1 | Classification of root cause of the incident under the incident types.  The following categories shall be considered:   * **Malicious actions** (if selected, choose one or more the following)   + Deliberate internal actions   + Deliberate physical damage/manipulation/theft   + Fraudulent * **Process**    + Insufficient and/or failure of monitoring and control     - Monitoring of policy adherence     - Monitoring of third-party service providers     - Monitoring and verification of remediation of vulnerabilities     - Identity and access management     - Encryption and cryptography:     - Logging.   + Insufficient/unclear roles and     - ICT risk management process failure:     - Failure in defining accurate risk tolerance levels     - Insufficient vulnerability and threat assessments   + Inadequate risk treatment measures   + Poor management of residual ICT risks * Vulnerability and patch management * Change management; * Capacity and performance management * ICT asset management and in-formation classification * Backup and restore; * Error handling;   + Inadequate ICT Systems Acquisition, Development, and Maintenance   + Insufficient and /or failure of software testing * **System**    + Hardware capacity and performance: incidents caused by hardware re-sources which prove inadequate in terms of capacity or performance to fulfill the applicable legislative requirements.   + Hardware maintenance: incidents resulting from inadequate or insufficient maintenance of hardware components, other than "Hardware obsolescence/ageing" as defined below.   + Hardware obsolescence/ageing: This root cause type involves incidents resulting from outdated or aging hard-ware components.   + Software compatibility/configuration: incidents caused by software components that are incompatible with other software or system configurations. It includes, but it is not limited to, incidents resulting from software conflicts, incorrect settings, or misconfigured parameters that impact the overall system functionality.   + Software performance: incidents resulting from software components that exhibit poor performance or inefficiencies, for reasons other than those de-fined under "Software compatibility/configuration" above. It includes incidents caused by slow response times, excessive resource consumption, or in-efficient query execution impacting the performance of the software or system.   + Network configuration: incidents resulting from incorrect or misconfigured network settings or infrastructure. It includes but it is not limited to incidents caused by network configuration errors, routing issues, firewall misconfigurations, or other network-related problems affecting connectivity or communication. Physical damage: incidents caused by physical damage to ICT infra-structure which lead to system failures.   + Other (please specify) * **Human**    1. Omission (unintentional)   2. Skills & knowledge: incidents resulting from a lack of expertise or proficiency in handling ICT systems or processes, that may be caused by inadequate training, insufficient knowledge, or gaps in skills required to perform specific tasks or address technical   3. Inadequate human resources: incidents caused by a lack of necessary re-sources, such as hardware, software, infrastructure, or personnel. It includes but it is not limited to situations where insufficient resources lead to operational inefficiencies, system failures, or an inability to meet business demands   4. Other (please specify) * **External**    1. Natural disasters/force majeure   2. Third-party   3. Other (please specify) |
| 4.3 | Information about the root causes of the incident  Description of the sequence of events that led to the incident including a concise description of all underlying reasons and primary factors that contributed to the occurrence of the incident.  Where there were malicious actions, description of the modus operandi of the malicious action, including the tactics, techniques and procedures used, as well as the entry vector of the incident.  Includes description of the investigations and analysis that led to the identification of the root causes, if applicable. |
| 4.4 | Information on whether or not and, if so, how legal requirements have not been complied with, or are likely not to be complied with, as a result of the major incident, including information on what requirements are affected. |
| 4.5 | Information on whether or not and, if so, how contractual arrangements and service level agreements with financial counterparts have been breached or are likely to be breached leading to non-compliance with contractual obligations as a result of the major incident. |
| 4.6 | Description of the measures and actions taken for the permanent resolution of the incident  The description shall include the following points in your answer (non-exhaustive list):   * Actions taken to permanently resolve the incident (excluding any temporary actions) * For each action taken, indicate the potential involvement of a third-party provider and of the financial entity * Indicate if procedures have been adapted, following the incident * Indicate any additional controls that were put in place or that are planned with related implementation timeline.   Potential issues identified regarding the robustness of the IT systems impacted and/or in terms of the procedures and/or controls in place, if applicable.  Financial entities shall clearly indicate how the envisaged remediation actions will address the identified root causes and when the incident is expected to be resolved permanently. |
| 4.7 | Assessment of the effectiveness of the actions taken and lessons learned |
| 4.8 | Date and time when the incident was resolved and the root caused addressed |
| 4.9 | Information if the permanent resolution date of the incidents differs from the initially planned implementation date |
| 4.10 | Information relevant for resolution authorities |
| 4.11 | Reclassification of the incident from major to non-major |
| 4.12 | Reasons for the reclassification |
| 4.13 | Materiality threshold for the classification criterion 'Economic impact' |
| 4.14 | Amount of gross direct and indirect costs and losses |
| 4.15 | Amount of expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft |
| 4.16 | Amount of replacement or relocation costs of software, hardware or infrastructure |
| 4.17 | Amount of staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff |
| 4.18 | Amount of fees due to non-compliance with contractual obligations |
| 4.19 | Amount of customer redress and compensation costs |
| 4.20 | Amount of losses due to forgone revenues |
| 4.21 | Amount of costs associated with internal and external communication |
| 4.22 | Amount of advisory costs, including costs associated with legal counselling, forensic and remediation services |
| 4.23 | Amount of other costs and losses |
| 4.24 | Amount of financial recoveries |
| 4.25 | Details related to the economic impacts |

## Response to information security incidents

The response to information security incidents must include at least the following

* Escalation, if necessary, including crisis management activities and possible use of business continuity plans;
* Ensure that all remediation activities performed are properly logged for later analysis;
* Analysis of available information, such as system, network and technical logs, as well as logs from relevant security products (e.g. malware protection software, data leakage prevention (DLP) and host and network-based IDS and IPS).
* Notification of the information security incident that has occurred or any relevant details to all relevant internal and external interested parties in accordance with the principle of "knowledge only if necessary";
* Coordinate with internal and external parties such as authorities, external stakeholders and forums, suppliers and customers to improve the effectiveness of the measures and minimize the impact on other organizations;
* Handling of necessary evidence (e.g. collection of evidence in accordance with legal requirements and protection against unauthorized manipulation)
* Investigating the causes of information security incidents with the support of specialists (e.g. experts in forensics and cyber incident response)
* Cooperation with IT specialists
* Containment and elimination of the information security incident (e.g. by making changes to access control systems, increasing network capacity, terminating or rerouting network connections or shutting down systems).

## Remediation of information security incidents

Recovery from information security incidents must include at least the following:

* Restoration of systems or networks (and supporting IT facilities) to a previously known safe state (i.e. the state they were in before the incident occurred)
* the recovery of information that has not been affected by the incident
* Closure of the information security incident.

## Follow-up and reporting of information security incidents

After recovery from information security incidents:

* checks must be carried out to determine the cause of the information security incident (e.g. through a root cause analysis)
* assessments must be carried out (with the involvement of the relevant specialist department and an IT specialist) to determine the impact of the information security incident on the company and to review the recovery measures implemented.
* If necessary, forensic investigations should be carried out (e.g. for legal purposes or in the case of serious information security incidents such as fraud)
* Identification and remediation of information security vulnerabilities, including vulnerabilities related to actions that caused, contributed to, or failed to prevent the incident.
* the existing security controls must be reviewed for their adequacy
* corrective measures must be taken to minimize the risk of similar incidents.
* the details of the information security incident must be documented in a post-incident report.

The notification of information security incidents must at least take the following into account:

* The Head of IT is responsible for the report. As far as possible, the Head of IT consults with the other members of the Data Protection, Information Security and IT Standards Committee before making the report.
* Serious data protection incidents must be reported immediately to the competent authority designated in Article 12 of Directive (EU) 2016/97;
* Serious security incidents (major incidents pursuant to DORA) must be reported immediately to BaFin on its reporting and publication platform portal [(](https://portal.mvp.bafin.de/MvpPortalWeb/app/login.html)https://portal.mvp.bafin.de/MvpPortalWeb/app/login.html), whereby the following deadlines must be observed:
  + Initial report within 4 hours of receiving information about an incident. In addition to the master data, the information to be reported includes all information in accordance with Chapter 3.1 of serial number 2
  + Complete report within 1 day (business day) of receiving information about an incident. In addition to the master data, the information to be reported includes all information in accordance with section 3.1 of serial number 3
  + Completion Report within 3 days (business days) after the incident is closed. In addition to the master data, the information to be reported includes all information in accordance with section 3.1 of serial number 4

Master data here are:

|  |  |  |
| --- | --- | --- |
| Number | Description | Value |
| 1.1 | Type of report | a) initial notification  b) Intermediate report  c) final report |
| 1.2 | Full legal name of the entity submitting the report | SÜDVERS Management Services GmbH |
| 1.3 | LEI of the entity submitting the report |  |
| 1.4 | Type of the entity submitting the report |  |
| 1.5 | Name of the financial entity affected |  |
| 1.6 | Type of financial entity affected |  |
| 1.7 | LEI code of the financial entity affected |  |
| 1.8 | Primary contact person name | Dirk Franken |
| 1.9 | Primary contact person email | [dirk.franken@suedvers.de](mailto:dirk.franken@suedvers.de) |
| 1.10 | Primary contact person telephone | 0049-761-45820 |
| 1.11 | Second contact person name | Alexander Meitinger |
| 1.12 | Secondary contact person email | [Alexander.meitinger@suedvers.de](mailto:Alexander.meitinger@suedvers.de) |
| 1.13 | Second contact person telephone | 0049-761-45820 |
| 1.14 | Name of the ultimate parent undertaking | SÜDVERS Holding GmbH & Co KG |
| 1.15 | LEI code of the ultimate parent undertaking |  |
| 1.16 | Name of affected third party providers |  |
| 1.17 | LEI code of affected third party providers |  |
| 1.18 | Reporting currency | Euro |

In addition to the reporting requirements regarding a serious security incident, a consolidated annual report must also be submitted, which must be structured as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of financial entity** | | |  | | |
| **Start and end date of accounting year of the financial entity** | | |  | | |
| **Reporting currency** | | |  | | |
| **Number of incident** | **Date of the submission of the final incident report** | **Incident reference number** | **Gross cost and losses of the incident in the accounting year** | **Recoveries of the incident in the accounting year** | **Net costs and losses of the incident in the accounting year** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **...** |  |  |  |  |  |
| **Aggregated annual costs and losses** | ----- | ----- |  |  |  |

* Non-serious cyber threats can be reported voluntarily to the competent authority.