Your ISMS and the Coronavirus

Information security management during the Coronavirus pandemic (as of 06 January 2021)

With this document we address *all* companies with an information security management system (ISMS). We describe how your ISMS can help your company to better manage the current sitation caused by the Coronavirus pandemic.

For TISAX participants in particular, we additionally provide pointers to some of the VDA ISA requirements that are especially important.

Please note:

For the more organisational levels of questions about TISAX we provide a more detail-oriented document. It contains the answers to questions specific to the current situation.

TISAX and the Coronavirus
Information for TISAX assessments during the Coronavirus pandemic (as of 06 January 2021)
https://portal.enx.com/tisax-handling-sars-cov-2_en.pdf

1 The information security management systems as a tool

The health and safety of employees is a top priority for every company, also with regard to information security. This is fully in line with the objective of information security, which is to protect all critical business processes of the organisation and its partners with regard to confidentiality and integrity, but also availability.

The novel Coronavirus (SARS-CoV-2) is a threat to persons as essential information carriers and as the basis of many critical business processes in the company. It is therefore not only necessary to maintain the management of information security in the current situation. Rather, an appropriate management system (ISMS) is to be understood, especially in this situation, as one of the essential control instruments for the executive board and management. It supports the decision makers in making informed and strategically correct decisions in every situation and then acting with the right priorities.

2 Assessment of the changed risk situation

The first step is to assess the changed risk situation caused by the coronavirus pandemic – especially with regard to availability – and to derive and correctly prioritise necessary actions. The threat posed by the coronavirus creates direct and indirect risks for the availability of persons:

1. Direct: Absence due to illness
2. Indirect: Illnesses and events in the social environment as well as government protective measures (e.g. restriction of freedom of movement), which result in the person not being available or only being available to a limited extent.

A reassessment of risks on the basis of a changed threat situation and measures derived from this is not only a regular but an absolutely necessary process and is explicitly demanded in the corresponding VDA ISA question 1.4.1. An example of this is the offer or even the order to shift work to the home environment in order to protect persons, prevent the spread of the disease, but also to reduce the risks with regard to the availability of persons.

3 TISAX-compliant implementation of measures

This means continuing to assess the associated risks before implementing measures and, if necessary, deriving additional measures with the right priority. VDA ISA question 3.1.2 aims to take into account the increased risks in terms of confidentiality and integrity of information, e.g. due to processing in the employee's home, even in crisis situations.

In order to be TISAX-compliant, at least the following aspects must be considered:

- Is working from home adequately regulated (question 1.1.1) and are the rules sufficiently well-known (question 2.1.3)?
- Do the rules for using mobile devices (questions 2.1.4 and 3.1.4), the rules for off-premises use of assets (question 3.1.3), the transport of information (question 1.3.2) and the handling of mobile storage devices (question 3.1.4) meet the requirements for work in the home office?
- Are suitable secure means of communication available? In particular: Do the means used have the necessary capacities and availabilities (question 5.3.2) and at the same time the necessary security features (question 5.1.2)?
- Are there any agreements with business partners which concern and/or restrict the taking or carrying out of work from the home office (question 7.1.1)? Does the business partner have to be informed separately about the shift or even the agreement has to be adapted?
- For all these points one should always take into account the risk that unnecessary or impracticable demands are not or insufficiently followed by the persons concerned and de facto weaken security. In this respect, the necessity and practicability should always be taken into account when assessing regulations.

This list makes no claim to completeness. You must also consider aspects beyond this in an appropriate manner.

Published by

ENX Association
an Association according to the French Law of 1901,
registered under No. w923004198 at the Sous-préfecture of Boulogne-Billancourt, France.

Addresses
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany

Contact

tisax@enx.com

+49 69 9866927-77

Version

Date: 2021-01-06, Version: 1.5

Classification: TISAX participants, ENX doc ID: n/a

Copyright notice