Information security policy (summary)

Information technology (IT) and information management (IM) are ubiquitous terms these days. Almost all business processes depend on quality and continuity of IM and IT. This is also the case for our primary process, secondary processes as well as supporting processes like financial mangement or human resource management. Without operational IT there can be no services for customers, no research, no production, no invoicing, no autorisation, etc.

The KB as a national library holds the value that all stakeholders should be able to trust the information as it is provided. In a time of increasing cybercrime, sometimes outright cyber-warfare, misinformation and the growing risk of being locked up in an information bubble by tech giants like Google and Facebook, the availability of trustworthy information sources might be more important than ever.

This is why it is evident that the management top carries out responsibility for IM and IT. No one other than the board has the ultimate responsibility. The board is not only responsible for implementation and governance of IM and IT but also for the safety and continuity of it. The latter is what is concerned when we talk about information security. This is the subject of our security policy.

Information security is directly related to the mission and priorities of the organisation. The priority that is given to information security reflects the business impact that security leaks can have: a business case is always involved when setting priorities. The concept of risk analysis is used to weigh risks and business cases and is used as input for determining fitting security structures and measures.

Information security concerns all IT and information resources and processes. Mainly 3 aspects are important to consider:

1. Availability: are resources/processes operational, are they online?
2. Integrity: is the content of informationflows secured, that is to say: can we be certain that it has not been tampered with and also can not be tampered with?
3. Confidentiality: is access to certain information only provided to people who are authorised and is it indeed inaccessible or unreadable to others?

Another aspect that is important to all of these other aspects is verifiability: we should not only make sure everything is fine now but also be able to verify this afterwards.

Information security can not be considered a primary or secundary process, not core business but if we do not take care of it, this will be to the detriment of core business. Information security as such is a first category business enabler. Therefore the board wants to ensure good governance, including auditing and feedback. We call this I-governance. It is crucial and management commitment is therefore indispensible.

The content of the information security policy is established by the executive council of the KB, supported by the management board and is valid for the whole organisation and all people involved in it whatsoever their function.

Management commitment is necessary but not sufficient. Information security is explicitly a responsibility of everyone involved. This notion will be propagated using formal means as well as by raising awareness. A special task is appointed to the middle managers who are made responsible for preconditionally and curatively enforcing the security policy.

To summarize: information security will funcion best when the whole organisation is involved. This is an ongoing process. This policy forms the groundwork for this. It descibes not only the abovementioned aspects but also which roles should be assigned, how information security is part of the Planning and Control cycle, how security incidents are handled (or better: prevented), which legal preconditions apply, etc.

There are a number of roles that can be considered crucial:

- The security coordinator (the corporate information security officer or CISO) of the KB: this is a role on the strategic level. The officer Security Coordinator is placed under the CIO and as such has access to the board. He has no operational responsibilities. The tasks assigned to him are guarding information security, asking difficult questions, preparing for audits and drafting policies and recommendations.
- The information security manager (ISM) who operates on the tactical (and operational) level. This role is the linking pin between the strategic level of the CISO and the day-to-day implementation and enforcement of the information security policy. This role is carried out by the security architect of the Information policy department.
- CSIRT-KB: the computer security incident response team of the KB, to be considered as the ‘fire department’ of information security and just as the real fire department tasked with both prevention and protection.