Data security principles

Den Haag • 00 maand jaar

PostNL Group Policy Cyber Security Management

3. Management ensures that cyber security related business risks are mitigated.

Management of a PostNL Group company is required to assess risks related to cyber security for all business processes and its (personal) data including new projects. Management of a PostNL Group company is responsible for the risk strategy and formally accepts the residual business risks and escalates when this exceeds their mandate.

https://postnl.sharepoint.com/sites/MgdShrdExIn01/gp/Paginas/Cyber-Security-Management.aspx

PostNL Group Policy Cyber Security Management

4. Management ensures that measures are taken to control and protect business information.

To ensure adequate data protection, management of each PostNL Group company is responsible for classifying business data and systems in terms of confidentiality, integrity and availability to avoid uncontrolled dissemination resulting in damage. This is valid from the moment that data is captured till the moment that data is purged.

The secure preservation of documents or data (e.g. from its creation until the destruction) is recorded in the PostNL Group procedure on data security.

https://postnl.sharepoint.com/sites/MgdShrdExIn01/gp/Paginas/Cyber-Security-Management.aspx

Summary:

Data security principles

1. All data has an owner
2. All data owners are responsible for classifying their information with regards to confidentiality, integrity, availability (and privacy, red.)
3. Management is responsible to perform risk management
4. Management is responsible for all the necessary protective measures, or other treatment of risks such as acceptance or avoidance.
5. The above is valid for the whole data cycle (from creation, to destruction of data).