data classification policy

Information Security Lead
first edition April 2021
revised edition August 2025

Adopted by the Board of Directors in Akelius Residential Property AB (publ) 2026-06-30

need

Akelius needs to protect sensitive and confidential data.

Data classification is critical for implementing appropriate protective measures.

essentials

The data classification policy applies to all users authorized to access Akelius' data.

Establish a framework for classifying Akelius data based on

- level of sensitivity
- value
- regulatory requirements
- criticality

Classification of data supports determining baseline security controls for data protection.

consider classification standards

Data classification is based on the level of sensitivity and the impact on Akelius if the data becomes public.

Depending on the level of sensitivity,
consider if the data should be

- disclosed
- altered
- destroyed

The classification helps determine what baseline security controls are appropriate.

classification into three levels

All Akelius data should be classified into one of the following three sensitivity levels.

public data

- can be published without negative consequences
- is the least sensitive data,
  with no expectation for privacy or confidentiality

Always handle all Akelius information with care.

internal data

- can be used by all employees and authorized externals
- is not intended by the data owner to be published or disclosed externally
- is protected by contractual obligations

confidential data

- is sensitive business information,
  unauthorized exposing may cause damage to the business
- is legally regulated and protected by law
- is data that would provide confidential or restricted information

how to handle and control classified data

There are no restrictions for public data.
Always handle your and Akelius' data with care.

act according to the need-to-know principle

Data access should be restricted,
so that you can only access information that you need for performing your work duties.

You should not have access to confidential information that you do not need.
The need-to-know principle prohibits access.

Should you still have access to such information, contact the system owner or IT service desk.

Delegation rules should be clearly defined.
Access for delegated persons should be temporary.

The sensitivity level of data determines how to handle and secure data.

	internal data	**confidential data**
data access and control	- Akelius staff - non-staff who have a business need to know	- accessible only to individuals with approved access - externals only with signed non-disclosure agreements - on a business need-to-know basis
transmission	strongly recommended through - Akelius network - VPN	- only permitted through the Akelius network, VPN, or remote desktop in other networks

	- remote desktop strongly discouraged for - guest, home, or public networks - public internet, email, instant messaging, text messaging	- use only authorized tools - encrypted - to the right persons Prohibited for - guest, home, or public networks without Akelius VPN - public internet, email, instant messaging, text messaging
storage	- encouraged in approved applications or authorized storage media and drives	- only in approved applications - authorized storage media and drives
backup and recovery procedures	strongly recommended	required
data retention policy	required	required
audit controls	the system owner is accountable for implementing procedures to periodically - monitor data access and records - review their systems for potential misuse, unauthorized access	the system owner is accountable for implementing procedures to actively - monitor data access and records - review their systems for potential misuse, unauthorized access

use supported tools and legal templates

find relevant documents on the intranet

Learn more about Akelius' retention policy here.
You can always find the latest document on the Intranet.

To use the non-disclosure agreement template, contact legal@akelius.com.

Use Microsoft Purview Information Protection to classify Office and PDF files.
Learn more about Microsoft Purview Information Protection here.

Learn more about working in the Akelius network & VPN from an external location here.

avoid use of tools not supported and recommended

For example, not supported and not recommended to use for any business related data

- public internet
- external media, like USB sticks
- non-business email address
- Short Message Service, SMS
- WhatsApp

You can use all applications provided by Technology.

disposal of information assets

Retain information in electronic format, as well as in physical format, for a predefined period in accordance with Akelius' retention policy.
Always comply with legal and regulatory requirements.

Use document distractions like shredders or certified data bins.
For electronic media, open a IT service desk ticket.

privacy and security team verify policy compliance

any exception to be approved in advance

Any exception to the policy must be approved in advance by the system owner, legal, or the privacy and security team.

severe consequences for non-compliance

Violating the rules, you may be subject to disciplinary action.

appendix - document history tracking

version	3
approval date	2026-06-30
status	final
classification	internal
document owner	Information Security lead
next revision	2027-06-30

version	date	changes	changed by
1	2021-04-01	new policy	Christian Öhlmann
2	2023-06-20	revised for ISO27001	Savvas Panayiotou
2	2023-07-20	approval	Igor Rogulj
2	2024-05-28	reviewed only	Savvas Panayiotou
2	2024-05-28	approval	Igor Rogulj
3	2025-08-21	formatting updates, hyperlinks	Christoforos Charalampidis
3	2025-08-27	approval	Igor Rogulj
3	2026-06-22	reviewed only	Christoforos Charalampidis
3	2026-06-30	approval	Board of Directors