Cybersecurity policy (BAsic)

 Template

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check**  |  |
| Author  |  |
| Owner |  |
| Date created |  |
| Last revised by  |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date of approval** | **Approved by**  | **Description of change** |
|  |  |  |  |

# Intro

**[Organisation]** recognises the crucial role that information plays in today's business objectives. In a modern world, information systems need to be highly interconnected and accessible from anywhere. While this presents great opportunities, the risk of hostile attacks or data loss is rapidly increasing.

This Cybersecurity Policy defines the minimum requirements applicable to all departments of **[Organisation]** so that we protect our intellectual property, our commercial advantage and our people from the consequences of poor Information Security and any cyber-attacks.

Naturally, due consideration is also given to respecting laws and regulations.

Where applicable, departments can define additional guidelines and take additional measures to ensure the required level of security.

# Policy principles

**We have effective policies and procedures in place**

We are aware of information security risks. We create security policies and procedures together. We know who is responsible and how we apply rules and procedures.

**We know our environment and manage risks**

We have an understanding of which information systems are important to [Organisation]. We know the risks of these systems and maintain them at acceptable levels. A continuous improvement cycle ensures that our security levels continue to adapt to changes in our organisation and environment.

**We build secure products and/or services**

[Organisation]'s products and services are built, tested and maintained with cyber-security and privacy in mind.

**We maintain a robust infrastructure**

The infrastructure on which vital systems depend is designed for high availability.

**We act proactively**

We patch regularly. We understand vulnerabilities in our infrastructure and keep abreast of newly discovered vulnerabilities. We learn from security events and incidents.

**We handle personal data properly.**

We collect, use and store personal data in accordance with the AVG ((EU) 2016/679). This means that we provide the necessary technical and organisational measures.

# Scope

In general, this Cybersecurity Policy applies to all information and systems of **[Organisation],** together with...

... the information systems they provide,

... the people (internal and external) who process it,

... the devices used to process it,

... the procedures on which it depends,

... the locations where we work

... the other aspects that may pose a risk.

Critical and confidential information or systems is information or systems that will harm the organisation if its confidentiality, integrity or availability is compromised.

# Minimum requirements

Our environment is managed in a way that contributes to cyber security.

This includes that:

* Roles and responsibilities related to cybersecurity are defined and communicated to both internal and external stakeholders.
* An inventory is made and maintained of all physical devices, systems and software used within the organisation.
* Equipment essential to critical systems must be properly maintained to ensure its continued availability and integrity. Maintenance contracts or spare parts should be considered.
* Antivirus, -spyware or other -malware programmes approved by the organisation should be installed and updated on the systems and endpoints identified by the organisation.
* The corporate network will be secured according to the requirements laid down in the network security policy.
* Operating systems for both clients and servers and applications will be provided with the necessary patches and security updates as described in the Policy around managing vulnerabilities and patches.
* Our employees and subcontractors are regularly made aware of the cyber risks and threats they may face and how to react when they come across suspicious activity. **The 10 golden rules for cyber security** are communicated and every employee or subcontractor must agree to abide by these rules.
* Sound Access Management is in place with due consideration of;
	+ Multifactor Authentication.
	+ Minimum access. Detailed policies are described in the Access Policy.
	+ Sufficiently strong passwords Detailed policy is described in the Password Policy
	+ Critical and confidential systems should at least successfully log on and off.
* There should be a process to recover critical systems in the event of a disaster. There should be a process to restore critical documents or records if they are accidentally deleted. Detailed policies are described in the Backup and Recovery Policy document.
* A response plan should be in place in the context of cyber incidents.

This policy document is part of a set of policy documents that support **[Organisation]** in establishing a sound cybersecurity strategy.