Technical and organizational security

Dynamicweb Software A/S – organizational and technical security policy
April 1st 2018

1. INTRODUCTION

This information security policy outlines Dynamicweb' approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the company's information systems.

Dynamicweb is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Dynamicweb is responsible.

2. TECHNICAL SECURITY MEASURES

2.1 Network and data communication

All data communication networks with external access are protected with a central firewall. Networks are configured and separated in different zones for functionality and usage. Networks used for customer hosting are protected by redundant hardware and access-lists.

Networks firewall, SSL Certificates and Virtual Private Network is used when personal data is accessed over the Internet.

2.2 Antivirus and patch management

Antivirus software is installed on all personal computers and servers. Incoming and outgoing emails are scanned for virus and spam. All computers used by Dynamicweb employees is automatic updated by central patch management and software updates, to ensure known security issues cannot be used to gain unauthorized access to systems and data. Servers used for customer hosting are part of weekly service window to ensure security updates are applied.

2.3 Backup and restore

All systems used for production environment must at least have a daily backup configured. By default, 14 days' point in time restore is available.

2.4 Delete and destroy

Personal Data should only be stored in our IT systems as long Dynamicweb and the partner or customer has an active agreement. Dynamicweb will ensure that data is deleted or at least personal data is removed when an agreement has expired in accordance to our Data Processing Agreement.

2.5 Monitoring and alerts

Critical systems are monitored 24/7/365 with notification and alerting to Dynamicweb Operations or Infrastructure suppliers.

3. ORGANIZATIONAL SECURITY MEASURES

3.1 Access control

All users, employees, customers, partners and sub-suppliers with access to IT systems controlled by Dynamicweb or hosting suppliers, is registered in Active Directory. Different domains are used for access to internal systems, Dynamicweb Cloud and Hosting servers.

User passwords has a maximum age of 90 days, where after the users must change password. Passwords must meet complexity requirements with a minimum length of 8 characters.

3.2 Confidentiality

Dynamicweb will assure confidentiality of information processed by Dynamicweb or sub-suppliers. Information is protected against any unauthorized access. Integrity of information shall remain intact.

3.3 Logging

Active Directory and IT systems is configured to ensure logging of user behavior, authorized and attempts at unauthorized access.

3.4 Data breach

Dynamicweb will report any unlawful data breach of any data processed by Dynamicweb or by our third party data processors to relevant persons and authorities within 72 hours of the breach if it is apparent.