dynavox group

Doc. name	Doc. owner	Approved by	Doc. type	Rev	Approved	Status
Information Security Policy	Head of IT	Board	Policy	3.0	2025-07-15	Released

Information Security Policy

Part of Code of Conduct for Dynavox Group

This policy must be read by all employees and consultants with access to Dynavox Group systems and premises, and all employees must explicitly certify that they will comply with this policy

Contents

1 Purpose and scope

Dynavox Group's approach to information security management is risk driven and is based on a balance between the cost of risk handling and the benefit provided. This helps our company to prioritize information security initiatives to get the greatest benefit from our information security investments and to achieve our set business objectives.

This policy must be read by all employees and consultants with access to company systems and premises, and all employees must explicitly certify that they will comply with this policy.

The Dynavox Group CEO is accountable for information security and the Head of Information Technology is responsible for information security.

1.1. Principles

To protect Dynavox Group, its employees and business partners from an information security perspective we enforce the following principles:

Awareness – All employees and consultants should be aware of the need for security of information systems and networks and what their role is in keeping the information secure.

Confidentiality – information is not disclosed or made available to unauthorized individuals, entities, or processes.

Integrity – information is complete and accurate.

Availability – information is accessible and usable when required.

2. Our commitment

Dynavox Group is committed to:

- Continuously improve our information security management policies and processes to monitor and strengthen our information security posture and awareness.
- Maintain a risk driven Information Security Management System that is based on a balance between the cost of risk handling and the benefit provided.
- Assure that information security is not a blocker for innovation.
- Be compliant with information security requirements including laws, regulations, and other compliance requirements.
- Report regularly on information security issues, performance and engage in active dialogue with all relevant interested parties.

3. Your Responsibility

Information security is based on common sense and sound judgment and this policy emphasizes that the contribution from each employee, consultant, and contractor is crucial; we trust you to take your responsibility as follows:

- Read this policy, seek clarifications where needed and comply.
- Manage information, IT equipment and services in accordance with the *IT Acceptable Use Policy* (internal only) .
- Partake in information security and privacy awareness training provided to you.
- Be vigilant about phishing and social engineering attempts. Always verify email senders and avoid clicking on links or opening attachments from unknown sources.
- Report any observed or suspected information security incident, incident risk, vulnerability or near miss to the IT service desk immediately.
- Share your ideas on how to improve information security.
- If you work in an IT role or administer any IT or related service, you will have additional specific expectations as outlined in the appropriate section of the *IT Policies and Acceptable Use* document.

2 Confidentiality classification and handling

Dynavox Group classifies and manages information assets as described in the Information Policy.

You are responsible to familiarize yourself with this classification matrix for confidentiality and the rules on how information may, or may not, be shared and handled. If uncertain, treat any information as Strictly Confidential unless confirmed otherwise. Public release of information is generally made by Executive staff or designated roles within the company, such as marketing and communications.

Do not share information with anyone without first ascertaining whether the individual is authorized and that there is a justifiable business reason.

3 Data protection

Any Personal Information collected, held, or processed by Dynavox Group relating to any individual is subject to the relevant provisions of applicable local law, including but not limited to Privacy regulations such as GDPR or HIPAA. The provisions set out in this policy are intended to serve as global guidelines and are therefore subject to any applicable local law provisions and/or staff policies governing the use of personal information in each jurisdiction where Dynavox Group operates.

- All personal data must be encrypted during storage and transmission. Encryption keys must be managed securely and limited to authorized personnel.
- Data retention policies must be followed, ensuring personal data is retained only for as long as allowed by applicable laws and regulations.
- If unsure about data handling, consult the Privacy Manager for further guidance.

4. Information security in the office

When working in the office follow the guidelines applicable for the office you are working in related to for example:

- ID badges
- Restricted zones
- Physical security/access control for systems
- Locking tablets/computers/workstations when you step away
- Check in/out of visitors and the use of visitor badges for guests
- Limit conversations for Confidential and Strictly Confidential information to conference rooms with closed doors

5. Information security outside the office

When working outside the office and particularly in public places you should exercise special care, such as:

- Never leave any equipment unattended. Keep your computer as hand luggage when travelling by plane.
- Discretely type in passwords and pin codes.
- When working in a public place, ensure that no one else is looking at your screen and never open confidential documents.
- If you travel and work on trains or planes you should use a screen filter when working with Confidential material (per the classification in Chapter 4)
- Be careful when talking to other colleagues in public places. Speak in a low voice and never discuss confidential information.
- Employees using personal devices for work purposes must:
- Install and maintain company-approved endpoint protection software.
- Ensure their devices are secured with strong passwords and encryption.
- Avoid storing "Confidential" or "Strictly Confidential" information locally on personal devices unless approved by IT.
- Report any loss or theft of personal devices used for work to IT immediately.

6. Reporting of information security incidents and risks

An information security incident is any event that has already compromised or has the potential to compromise the confidentiality, integrity, or availability of Dynavox Group information in any format, or any IT system or service. This includes physical information security incidents.

You must report any observed or suspected information security incident or incident risk to the Global IT service desk immediately.

Vulnerabilities and near misses are included in the definition of an information security incident and must also be reported.

It is better to report too much than too little. If you are not sure, report it anyway.

7. Audits and Assessments

Audits of information, systems and services will be performed as needed to ensure an accurate assessment of the effectiveness of the organization's safeguards, systems, and procedures. Additionally, audits may be performed on employee usage of Information Services and Systems to ensure compliance.

It is mandatory to report any observed or suspected information security incident, vulnerability, or near miss immediately using the provided reporting mechanisms.

All employees, contractors and suppliers are expected to comply and assist with the audits and assessments when asked. Hindering or failure to fully support and comply is not acceptable.

8. References to associated policies

- Information Policy
- IT Acceptable Use Policy (internal only)
- Privacy Policy (internal only)