EUROPEAN
DENTAL GROUP

CYBER SECURITY POLICY

The way we care

For our Patients, People and Environment

1. INTRODUCTION

Our company Cyber security policy outlines our guidelines and provisions for preserving the security of our data and infrastructure.
The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

1.1 Scope

The EDG Cyber security policy applies to all our employees an representatives, regardless of their employment or position within the organization. The management of each operation subsidiary of EDG is responsible for ensuring that this Cyber security policy is implemented and adhered to in to the Group's business activities.

All employees of EDG are responsible for ensuring that they personally and the entity at which they are employed act in accordance with this policy.
EDG act according (inter)national and European legislation and guidelines.
National legislation and guidelines need to be compliant with international standards applicable. Where there is a discrepancy between the applicable national legislation and guidelines and they conflict with this policy, you must apply the strictest standard.

2. POLICY ELEMENTS

2.1 Confidential data

Confidential data is secret and valuable. Common examples are:

- Customer/Patients lists (existing and prospective)
- Data of customers/patients/partners/vendors
- Unpublished financial information
- Patents, formulas or new technologies

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Data should be classified in confidential and non-confidential data. Confidential data should be stored on the company network / devices, and not on personal devices, USB's or other personal data carriers.

2.2 Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.
- Do not install software without checking with the IT department and be aware of malicious software.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment they are obliged to use the equipment properly and maintain it in good working order. They have to keep it secure as described above.

2.3 Email

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

- All use of email must be consistent with EDG policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- EDG email accounts should be used primarily for EDG business-related purposes; personal communication is permitted on a limited basis, but non-EDG related commercial use is prohibited.
- All EDG data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- Email should be retained only if it qualifies as a EDG business record. Email is a EDG business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a EDG business record shall be retained according to EDG Record Retention Schedule.
- The EDG email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any EDG employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding EDG email to a third party email system. Individual messages which are forwarded by the user must not contain EDG confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct EDG business, to create or memorialize any binding transactions, or to store or retain email on behalf of EDG with patient data or sensitive company data.

- Using a reasonable amount of EDG resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a EDG email account is prohibited.
- EDG may monitor messages for cyber security reasons without prior notice.

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

If an employee isn't sure that an email they received is safe, they can refer to the IT Department.

3. MANAGE PASSWORDS PROPERLY

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters).
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their personal passwords every three months.

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the local IT Department. Whenever possible, the use of multi-factor authentication is obliged.

4. TRANSFER DATA SECURELY

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer/patient information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT Department for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.

Our IT Departments need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our IT Departments. Our IT Departments must investigate promptly, resolve the issue and send a companywide alert when necessary.

5. ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to [HR/ IT Department].
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems to the IT Department.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media policy.
Our IT Departments should:

- Follow the EDG security guidelines based on the CIS framework and the Nordic security Must Do’s.
- Define roadmaps to continuously improve security.

EDG will provide security training for all employees, which will be obliged to follow on a regular base. The training will focus on following items:

- European Dental Groups own policies /code of conduct on how to handle data and data sources
- Basic security awareness training
- Privacy
- AVG / GDPR (and, if applicable, other compliance training like ISO27001 etc.)
- Handling personal/sensitive data
- Recognizing phishing (red flags in emails, attachments and links)
- Recognizing social engineering
- Safe password use
- Safe browsing
- Safe data storage / use of cloud applications etc.
- Using email securely
- Using social media securely
- Using mobiles securely

EDG will set up a SOC (Security operation centre) that monitors all activity in the companies infrastructure on malicious activities. This is an important measure to monitor and improve the security of EDG, and to help EDG with resolving (major) security incidents.

6. REMOTE EMPLOYEES

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.
We encourage them to seek advice from our IT Departments.

EUROPEAN
DENTAL GROUP