

Security Policy



As a modern, forward-looking business, PhoenixDX recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, PhoenixDX has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognised best practice.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- Access control
- Asset management
- Communications and operations security
- Human resources security
- Information systems acquisition, development and maintenance
- Physical and environmental security
- Risk assessment

We don't just rely on written security policies or standards when it comes to information security. We also uphold the confidentiality, integrity and availability of information through safeguarding our technological assets and resources. Measures consist of not only, but also:

- Multifactor authentication approaches
- Antivirus and anti-malware software
- Desktop and laptop full disk encryption
- Monitoring and detection systems

Training and awareness programs

In the face of ever-changing attack methods, we are constantly updating information, guidance and training for PhoenixDX employees. Raising awareness of threats to data privacy and information security is an ongoing and dynamic process. This is a process we take very seriously, not only in the mandatory training that is regularly updated for professionals in each PhoenixDX service line, but also in many other activities to raise awareness across the organization.

Business continuity and disaster recovery

Our dedication to safeguarding organization and customer data is illustrated through our disaster recovery and business continuity capabilities. We are committed to ensuring PhoenixDX's people, business processes, offices, applications and data in the event of a catastrophic event. The disaster response and system recovery procedures for our critical services applications have been carefully planned and tested. Our disaster recovery and business continuity methods include:

- Business Impact Assessments
- Mission-critical disaster recovery plans
- Disaster recovery and business continuity plans are periodically tested to verify the integrity

Supplier risk assurance program

PhoenixDX adopts a risk based approach to end to end supplier assurance to ensure our suppliers are “Fit for Business” and “Fit for Purpose” by:

- Evaluation of prospective suppliers for compliance with our ISO 27001 policies and controls
- Performing basic assurance checks including preparation of risk ratings and findings
- Mitigation of risk findings

You can consult more information on our security portal [here](#) or you can contact us at security@phoenix-dx.com.