

Security policy

Our approach

- Our ambition is to ensure zero harm from security incidents
- We work continuously to safeguard Equinor's people, assets, and operations from security risks through a holistic approach
- We align our requirements and guidance with international security standards and best practices and comply with all relevant security legislation and regulations
- We use a common management model to maintain and develop our capability across physical, personnel and cyber security disciplines
- We have clear security objectives, that complement Equinor's Internal Control Framework

We are committed to

- Ensuring security situational awareness and identifying security threats and risks
- Engaging risk owners and relevant stakeholders in risk mitigation activities
- Preserving the availability, integrity and confidentiality of physical and electronic data and information throughout the organization
- Detecting, responding, recovering, and learning from security incidents

How we work

- We collaborate with internal and external networks of experts and react quickly to changing threats and threats landscape
- We require all our employees and hired contractors to comply with this policy and offer appropriate awareness training and competence development plans
- We implement security risk management throughout the value chain and in the Capital Value Process
- We continually improve our defenses, and security controls, through internal and external audits, reviews, exercises and tests
- We measure and monitor security performance and report regularly to the board of directors
- Consequences of breaches are handled according to Equinor's [Code of conduct](#)