Measures for Implementing the National Cyber Security Strategy 2025

A. Knowing cyber threats
- A.001 Updating the situational overview of cyber threats relevant to civil protection
- A.002 Preparing a situational overview of current cyber threats

B. International cooperation, collaboration, information exchange and networking
- B.003 Strengthening the exchange of information between the national authorities
- B.004 Creating a cooperation framework and deepening the collaboration between public bodies
- B.005 Enabling and establishing the exchange of information for the economy and the financial center
- B.006 Promoting the exchange of information among essential and important entities (critical infrastructure) and public bodies
- B.007 Expanding international cooperation
- B.008 Collaboration between public bodies and strategic partners and international organisations
- B.009 Positioning the cyber diplomacy of the Principality of Liechtenstein

C. Vulnerability and risk management
- C.010 Strengthening Liechtenstein's cyber capabilities to defend against attacks
- C.011 Expanding central vulnerability monitoring and the provision of information
- C.012 Developing capabilities and competencies in connection with vulnerability monitoring at financial intermediaries and critical infrastructures
- C.013 Identifying supply chain dependencies at critical infrastructures
- C.014 Supporting stakeholders in assessing cybersecurity in the supply chain
- C.015 Cybersecurity in public procurement
- C.016 Use of open source software and support for open source projects
- C.017 Establishing a tool for voluntary self-assessment (self-assessment and benchmarking)
- C.018 Creating framework conditions for the use of managed security service providers by the economy

D. Information, prevention and raising awareness
- D.019 Establishing an internet platform for awareness training and raising awareness
- D.020 Disseminating a cyber hygiene guide for the population and SMEs
- D.021 Creating an overview of technical and regulatory developments
- D.022 Raising awareness of cybersecurity among all stakeholders
- D.023 Establishing best practices and techniques for crisis management

E. Education and training, research
- E.024 Strengthening research and education in the field of cybersecurity within the economy, the financial center and critical infrastructure
- E.025 Promoting education and training
- E.026 Promoting education and training within public bodies
- E.027 Establishing a National Cybersecurity Innovation Hub
- E.028 Supporting cybersecurity startups

F. Incident response and crisis management
- F.029 Establishing a national crisis organisation for managing large-scale cybersecurity incidents and crises
- F.030 Involving stakeholders in the national crisis organisation
- F.031 Strengthening cooperation with platforms and internet service providers
- F.032 Conducting and participating in exercises
- F.033 Establishing a civil society response component for large-scale cyber events
- F.034 Building and expanding the incident response capabilities of critical infrastructure
- F.035 Creating a cyber emergency plan / point of contact for the population
- F.036 Supporting stakeholders with incident response by providing general assistance

G. Regulation, supervision and control
- G.037 Creating commitment through regular supervision of the financial center
- G.038 Creating commitment through regular supervision of essential and important entities (critical infrastructure)
- G.039 Timely implementation of EU cybersecurity regulations

H. Cybercrime and law enforcement
- H.040 Strengthening competencies for identifying the authorship of cyberattacks (attribution)
- H.041 Publishing a regular cybercrime situational overview