COUNTRY: **LITHUANIA**

Lithuania published a comprehensive cybersecurity strategy in 2011, however information on its implementation remains limited. The Lithuanian computer emergency response team, CERT-LT, covers all national networks, not exclusively government ones, and the State Information Resources Management Council acts as a powerful policy formation and management body.

The cybersecurity strategy recognises the value and need for public-private partnerships, but no formalised or systematic cooperation yet exist.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en> was adopted by the Lithuanian government in 2011. It is a comprehensive plan that includes an assessment of Lithuania's cybersecurity capacity and a set of clearly stated goals, which are mapped to an implementation schedule.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	◑	There is no discrete plan covering critical infrastructure in general. Critical information infrastructure is addressed in the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019. <www.ird.lt/viewpage.php?page_id=83&lang=en> The programme acknowledges the need for Lithuania to adopt a stronger regulatory framework for the protection of critical infrastructure that includes the implementation of a coordination structure between entities engaged with critical infrastructure, as well as testing and monitoring systems to facilitate the prevention of incidents.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en> addresses electronic information security in general, but also includes goals to improve the legal framework and processes that support information security generally. There is no specific requirement for written information security plans.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Law on the Management of State Information Resources 2011 <www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=432270&p_tr2=2> requires the regulatory body, the State Information Resources Council, to establish criteria for the government regarding information importance assessments, state information systems, and other information systems based on the importance of the information involved. The State and Official Secrets Act 1999 <www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=91654> dictates a system of classification for data, based on the potential harm caused to the state, its agencies, or its entities in the event that the data in question is disclosed. The classification system consists of four levels, each graded according to the degree of potential harm involved in the event of the data in question being disclosed. Assignment of any of the classification levels deems that the data in question a state secret. The act also lists the types of data that can be classified a state secret, however it does not require all data of the types listed to be classified. It should be noted that the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en > acknowledges that the legal framework supporting information security is fragmented and does not cover all member of the "information society".
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The State and Official Secrets Act 1999 <www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=91654> lists a four-tired classification system that is to be applied to data deemed a state secret. These classification levels are assigned according to the risk involved in the event of the disclosure of the data in question. The act subsequently maps security practices and requirements to these classification levels.

COUNTRY: LITHUANIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation or policy in place in Lithuania that requires (at least) an annual cybersecurity audit. There is a requirement in the Law on the Management of State Information Resources 2011 <www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=432270&p_tr2=2> that an audit of government information technologies be carried out at least once every three years, as part of the monitoring and assessment procedures of the law. Furthermore, there is a provision in Article 3 of the State and Official Secrets Act 1999 <www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=91654> that allows the State Security Department to monitor compliance with state secrecy classification, use, and storing procedures. This provision does not, however, identify a specific auditing process, nor does it require this process to be carried out within a specific timeframe.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	There is no legislation or policy in place in Lithuania that requires a public report on cybersecurity capacity for the government. The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf> contains a detailed assessment of Lithuania's cybersecurity capacity as of 2011 and requires an annual public report on the progress of the implementation of the programme's stated goals.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation in place in Lithuania that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	The Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services <www.cert.lt/doc/CERT_LT_rules[EN].pdf> requires that providers of public communications network are required to report certain types of security incidents. The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en> recommends implementing a stronger legal requirement for incident reporting, as part of a wider strengthening of the legal framework supporting electronic information security.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en> contains an appropriate definition for "critical information infrastructure".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en> contains a recognition that standards and certification processes in Lithuania are not yet mature, and it recommends that Lithuania develop international cooperation in the area of electronic information security (cybersecurity), including standards.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	The National Electronic Communications Network and Information Security Incidents Investigation Service (CERT-LT) <www.cert.lt> was established in 2006 under the name CERT-RRT. It is responsible for coordinating security and incident response measures across all Lithuanian networks.
2.	What year was the computer emergency response team (CERT) established?	2006	

COUNTRY: LITHUANIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
3.	Is there a national competent authority for network and information security (NIS)?	✔	The State Information Resources Management Council is responsible for the formation of policy, guidelines, and priorities with regard to state information. This includes document protection procedures and classification of documents according to importance of the data they contain. The duties of the council are set out in the Law on the Management of State Information Resources 2011. <www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=432270&p_tr2=2> The National Electronic Communications Network and Information Security Incidents Investigation Service (CERT-LT) <www.cert.lt> is the responsible authority regarding cybersecurity incidents in particular. From 1 January 2015 the new Lithuanian Law on Cyber Security defining the organisation of a cybersecurity system, its management and control, has entered into force. The Law designates authorities responsible for the development and implementation of cybersecurity policies and sets their competences, functions, rights and obligations. The law stipulates that the Ministry of National Defence has to formulate, coordinate and implement the organisation of the state cybersecurity policy. This includes the establishment of the National Cyber Security Centre, which was launched 1 January 2015.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-LT <www.cert.lt> is tasked with managing the reporting of cybersecurity incidents. CERT-LT provides an online reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Lithuania participated in the multi-national cybersecurity exercise Cyber Coalition 2013 organised by NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	The Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services <www.cert.lt/doc/CERT_LT_rules[EN].pdf> contains the provision, but not the requirement, for the authority to inform the Prime Minister and senior government and European Union officials in the event of a cybersecurity incident.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership) for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Lithuania.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there is no industry-led cybersecurity platform in Lithuania, Infobalt <www.infobalt.lt>, an association of Lithuanian ICT companies, engages with cybersecurity in the course of its operations.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf> recognises the need to encourage public-private cooperation, however no specific public-private partnership has been detailed.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Lithuania does not have sector-specific joint public-private plans in place.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been defined.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been released.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 <www.ird.lt/viewpage.php?page_id=83&lang=en> includes a comprehensive education plan and an implementation schedule. For example, the strategy includes a target of establishing 50 cybersecurity self-help websites by 2015.