# COUNTRY: **ROMANIA**

Romania has a somewhat vague cybersecurity strategy, adopted in 2013. Its legal framework is limited, although relevant legislative proposals have been submitted to the parliament for adoption. CERT-RO is the national computer emergency response team. It covers all users of Romanian networks. Furthermore, the cybersecurity strategy proposes the establishment of two other cybersecurity agencies.

| | QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|---|
| | **LEGAL FOUNDATIONS** | | |
| 1. | Is there a national cybersecurity strategy in place? | ✓ | The Cyber Security Strategy of Romania <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> was adopted in 2013. It provides clear definitions of key terms and concepts. It covers a broad scope, and its lines of action are high-level statements of intent that are not mapped to an implementation timeline. |
| 2. | What year was the national cybersecurity strategy adopted? | 2013 | |
| 3. | Is there a critical infrastructure protection (CIP) strategy or plan in place? | ✓ | Emergency Ordinance 98/2010 on the Identification, Designation and Protection of Critical Infrastructure 2010 acts as the critical infrastructure protection strategy for Romania. |
| 4. | Is there legislation/policy that requires the establishment of a written information security plan? | ✗ | There is no legislation or policy in place in Romania that requires the establishment of a written information security plan. |
| 5. | Is there legislation/policy that requires an inventory of "systems" and the classification of data? | ✓ | The Law on Protection of Classified Information 2002 <www.sri.ro/fisiere/legislation/Law_protection-classified-information.pdf> requires information relating to national defence and security, critical infrastructures and the foreign policy of Romania to be classified. This information is classified according to a three-tiered classification system set out in Article 18 of the law. The classification levels are assigned according to the risk involved in disclosing the classified information. |
| 6. | Is there legislation/policy that requires security practices/requirements to be mapped to risk levels? | ✓ | The Law on Protection of Classified Information 2002 <www.sri.ro/fisiere/legislation/Law_protection-classified-information.pdf> maps security practices and requirements to the assigned classification level of the information being handled. The classification levels are assigned according to the level of risk involved in disclosing the information. |
| 7. | Is there legislation/policy that requires (at least) an annual cybersecurity audit? | ✗ | There is no legislation or policy in place in Romania that requires an annual cybersecurity audit.<br>The Cyber Security Strategy of Romania <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> calls for a clear process of monitoring and reporting of government cybersecurity practices, however, it does not outline a specific auditing process. |
| 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 Romania that requires a public report on cybersecurity capacity for the government.<br>The Cyber Security Strategy of Romania <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> makes a general call for strengthening monitoring and reporting practices, but does not specifically call for a public report on cybersecurity capacity. |
| 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 or policy in place in Romania that requires each agency to have a chief information officer or chief security officer.<br>The responsibility for the protection of classified information is centralised in the Office for Protection of State Secrets, a branch of the Romanian intelligence service, the SRI. <www.sri.ro> |

## COUNTRY: ROMANIA

| QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|
| 10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents? | ◑ | There is no legislation or policy in place in Romania that specifically requires mandatory reporting of cybersecurity incidents.<br>Reporting of cybersecurity incidents is partially covered by the Law Establishing the National Security Incident Response Cybernetics — CERT-RO 2011 <www.cert-ro.eu/legislatie.php>, which compels providers of electronic communication networks (both public and private) to work with CERT-RO in fulfilling its duties to provide early warning, real-time information, and support on cyber-attacks. |
| 11. Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)? | ✔ | Emergency Ordinance 98/2010 on the Identification, Designation and Protection of Critical Infrastructure 2010 includes an appropriate definition for "critical infrastructure protection". <http://www.sri.ro/upload/Brosura%20IC%20ENG.pdf> |
| 12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements? | ◑ | The Cyber Security Strategy of Romania 2013 <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> includes a commitment to develop and promote standards in the future, and a broad commitment to international cooperation. The strategy, however, does not include instruction on the adoption of specific standards or certification requirements. |
| **OPERATIONAL ENTITIES** | | |
| 1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)? | ✔ | CERT-RO <www.cert-ro.eu> was established in 2011. It is responsible for the prevention of incidents and the coordination of incident response measures across all Romanian networks. |
| 2. What year was the computer emergency response team (CERT) established? | 2011 | |
| 3. Is there a national competent authority for network and information security (NIS)? | ✔ | The Romanian Intelligence Service, the SRI <www.sri.ro>, is the body responsible for the protection of state information and any network utilised by government entities in the possession of state secrets.<br>The Cyber Security Strategy of Romania <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> establishes two additional entities, which would act in conjunction to cover cybersecurity specific network and information security in Romania.<br>• The National Cyber Security System (SNSC) is a body composed of representatives from public institutions and would be tasked with the building and maintenance of a range of cybersecurity measures.<br>• The Operative Council for Cyber Security oversees the SNSC in its duties, as well as responding in the event of critical cybersecurity incidents. It is composed of representatives from Romanian government ministries and Romanian intelligence services.<br>While the Cyber Security Strategy of Romania was adopted in 2013, as of August 2014, it is unclear whether either of these bodies has formally commenced undertaking their duties. |
| 4. Is there an incident reporting platform for collecting cybersecurity incident data? | ✔ | CERT-RO <www.cert-ro.eu> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as having in place an online reporting structure to log cybersecurity incidents. |
| 5. Are national cybersecurity exercises conducted? | ◑ | Romania has participated in multi-national cybersecurity exercises organised by both the European Union and NATO. |

## COUNTRY: ROMANIA

| QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|
| 6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents? | ◑ | There is no clear national incident management structure for reporting cybersecurity incidents, however limited requirements that cover reporting exist in legislation.<br>The Law Establishing the National Security Incident Response Cybernetics — CERT-RO 2011 <www.cert-ro.eu/files/doc/HG_494-2011_CERT-RO.pdf> requires CERT-RO to maintain an early warning and real-time incident reporting system, and to engage with both public and private entities.<br>Furthermore, the Cyber Security Strategy of Romania <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> established two bodies, the National Cyber Security System and the Operative Council for Cyber Security, that have certain responsibilities in the event of a cybersecurity incident. The operative council is composed of representatives from Romanian government ministries and Romanian intelligence services. While the Cyber Security Strategy of Romania was adopted in 2013, as of August 2014, it is unclear whether either of these bodies has formally commenced undertaking their duties. |
| **PUBLIC-PRIVATE PARTNERSHIPS** | | |
| 1. Is there a defined public-private partnership for cybersecurity? | ✖ | There is no defined public-private partnership for cybersecurity in Romania. |
| 2. Is industry organised (i.e. business or industry cybersecurity councils)? | ◑ | There are no industry-led cybersecurity organisations in Romania. The Cyber Security Research Centre of Romania (CCSIR) <ccsir.org> is a non-governmental organisation committed to the development and research of cybersecurity. |
| 3. Are new public-private partnerships in planning or underway (if so, which focus area)? | ✔ | The National Cyber Security System (SNSC) is a body comprised of representatives from public institutions and would be tasked with the building and maintenance of a range of cybersecurity measures. |
| **SECTOR-SPECIFIC CYBERSECURITY PLANS** | | |
| 1. Is there a joint public-private sector plan that addresses cybersecurity? | ✖ | Romania 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 Cyber Security Strategy of Romania 2013 <www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf> includes a commitment to develop educational programs in the form of compulsory education on internet safety and computing equipment. |