

# IT Laws and Regulatory Bodies in Sri Lanka

---

## 1. Introduction

---

In today's digital age, where technology is integrated into almost every aspect of our lives, the threat of cyber-crime looms large. Sri Lanka, like many other nations, faces the challenge of combatting cyber threats and ensuring the safety of its digital spaces. As in many other countries, Digital Laws play a major role in Sri Lanka's ICT sector. These laws provide the necessary legal environment for using electronic data and digital documents for official as well as personal purposes and carrying out electronic transactions.

## 2. IT Laws in Sri Lanka

---

Sri Lanka has enacted several laws to regulate and govern information technology practices and ensure cybersecurity. Some of the key laws include:

1. Computer Crimes Act No. 24 of 2007: This act provides legal provisions to identify computer crimes and stipulates punishments for such offenses. It covers various cybercrimes such as unauthorized access, hacking, and data theft.
2. Electronic Transactions Act No. 19 of 2006: This act facilitates and provides legal recognition for electronic transactions. It establishes the legal framework for electronic signatures, electronic documents, and electronic contracts.
3. Intellectual Property Act No. 36 of 2003: While not specifically an IT law, this act includes provisions for protecting computer programs and software under copyright law.
4. Online Safety Act (proposed): This act aims to address issues related to online harassment, cyberbullying, and other forms of online abuse.

These laws have a significant impact on IT practices and cybersecurity in Sri Lanka. They provide a legal framework for prosecuting cyber criminals, ensure the validity of electronic transactions, and protect intellectual property in the digital realm. This legal environment encourages the growth of e-commerce and digital services while also safeguarding the rights and security of individuals and organizations in cyberspace.

### 3. Computer Crime Investigation Division (CCID)

---

The Computer Crime Investigation Division (CCID) is a specialized unit within the Sri Lanka Police that focuses on investigating and combating cybercrimes.

#### Tasks and Role of the CCID:

- Investigate computer-related crimes and cybercrimes
- Gather digital evidence for legal proceedings
- Provide technical assistance to other law enforcement units in computer-related investigations
- Conduct awareness programs on cybercrime prevention

#### Services Offered:

- Investigation of various cybercrimes, including hacking, online fraud, identity theft, and cyberstalking
- Digital forensics and analysis of electronic devices
- Assistance in tracking and apprehending cyber criminals
- Collaboration with international law enforcement agencies on transnational cybercrimes

#### Contact Details:

Computer Crime Investigation Division Police Headquarters, Colombo 01, Sri Lanka Phone: +94 11 2320141 Email: [ccid@police.lk](mailto:ccid@police.lk) (This is a hypothetical email address)

### 4. Sri Lanka Computer Emergency Readiness Team (SL CERT)

---

SL CERT is the national center for cyber security in Sri Lanka, responsible for coordinating defensive measures against cyber threats and disseminating information to protect ICT systems.

#### Tasks and Role of SL CERT:

- Coordinate incident response for cyber security incidents
- Provide proactive measures to prevent cyber attacks
- Conduct research and analysis on emerging cyber threats
- Raise awareness about cybersecurity among the public and organizations

#### Services Offered:

- Incident response and management for cyber attacks
- Vulnerability assessments and penetration testing

- Security audits and consultations
- Training and awareness programs on cybersecurity
- Threat intelligence sharing with relevant stakeholders

## Contact Details:

Sri Lanka CERT|CC No. 9, Centerpoint Building, 1st Floor, Independence Avenue, Colombo 07, Sri Lanka  
Phone: +94 11 2691692 Email: [info@cert.gov.lk](mailto:info@cert.gov.lk) Website: <https://www.cert.gov.lk>

## 5. Telecommunications Regulatory Commission of Sri Lanka (TRCSL)

---

The Telecommunications Regulatory Commission of Sri Lanka (TRCSL) was created under the Sri Lanka Telecommunication (Amendment) Act No. 27 of 1996. As the country's main telecom regulatory agency, TRCSL aims to support continuous growth in the telecom industry by guiding regulations, protecting the public, and adapting to a competitive market. TRCSL will make sure that market competition is open, fair, and effective.

### Vision

"To be recognized as a world leader in an advancing communication industry through scientific and regulatory excellence."

### Mission

"Ensure timely delivery of the service nationwide at an acceptable quality and affordable cost through promotion of fairness and justice in a competitive market through a skilled and ethical workforce."

### Objectives of TRCSL

- Ensure reliable and efficient national and international telecommunication services.
- Protect consumer interests regarding charges, quality, and variety of telecom services and equipment.
- Maintain and promote fair competition in the telecom industry.
- Support rapid and ongoing development of telecom facilities.
- Encourage research and development of new telecom technologies.

### Responsibilities of TRCSL

- Enforce the Act and license conditions for telecom operators.
- Promote fair and sustainable competition among licensed operators.

- Monitor competition to ensure operators meet public interest goals.
- Ensure seamless interconnection between networks and services.
- Create a transparent and easy licensing framework.
- Ensure telecom services are reasonably priced and affordable.

## Contact Details

Address: Telecommunications Regulatory Commission, No. 276, Elvitigala Mawatha, Colombo 08, WP, Sri Lanka  
General Email: [dgtsl@trc.gov.lk](mailto:dgtsl@trc.gov.lk) General Phone: +94 11 2689345, 1900 General Fax: +94 11 2689341  
Website: <https://www.trc.gov.lk> Consumer Complaint's Email: [cc@trc.gov.lk](mailto:cc@trc.gov.lk)

## 6. Conclusion

---

Sri Lanka has made significant strides in establishing a robust framework for regulating IT activities and maintaining cybersecurity. The country's IT laws provide a solid legal foundation for addressing cybercrimes and facilitating digital transactions. The three key regulatory bodies - CCID, SL CERT, and TRCSL - each play crucial roles in this ecosystem:

1. The CCID focuses on investigating and prosecuting cybercrimes, ensuring that the laws are enforced effectively.
2. SL CERT acts as the first line of defense against cyber threats, providing incident response and proactive measures to protect the country's digital infrastructure.
3. TRCSL regulates the telecommunications industry, ensuring fair competition and protecting consumer interests, which is crucial for the development of a secure and reliable digital environment.

Together, these laws and regulatory bodies create a comprehensive system for promoting cybersecurity, fostering innovation in the IT sector, and protecting the rights of individuals and organizations in the digital space. As cyber threats continue to evolve, it will be crucial for Sri Lanka to regularly update its laws and strengthen its regulatory bodies to stay ahead of potential risks and maintain a safe digital environment for its citizens and businesses.

### References:

1. [https://www.trc.gov.lk/pages\\_e.php?id=2](https://www.trc.gov.lk/pages_e.php?id=2)
2. Computer Crimes Act No. 24 of 2007
3. Electronic Transactions Act No. 19 of 2006
4. Intellectual Property Act No. 36 of 2003
5. Sri Lanka CERT|CC official website: <https://www.cert.gov.lk>