Ensuring a Quality Cybersecurity

In terms of Cybersecurity, the CDOs have the responsibility to follow the guidelines and standards provided by the NCSA and RISA. These guidelines are published on their respective websites or communicated directly to the CDOs.

CDOs also have to contact the appropriate authorities to intervene in case threats are detected, or to come to implement some cybersecurity guidelines. The CDOs responsibility covers the compliance with Regulations in terms of cybersecurity. He/she has to ensure that the department complies with relevant cybersecurity regulations and standards applicable.

Thus, the CDO must conduct regular Risk Assessment and Management. It involves conducting regular risk assessments to identify potential vulnerabilities and threats and develop a risk management plan to prioritise and mitigate these risks effectively.

The CDO also must conduct team members training and awareness by educating all department members about cybersecurity best practices. The CDO must conduct regular training sessions to raise awareness about phishing, social engineering, and other common cyber threats.

Another key action is the access control and authentication. It covers the implementation of strong access controls and authentication mechanisms. It enforces the principle of least privilege, ensuring users have access only to the data and systems necessary for their roles.

Some Regular Updates and Patch Management are necessary. The CDO must keep all software, operating systems, and security tools up to date with the latest patches and updates as vulnerabilities often arise from outdated software versions.

The CDO and his/her team must secure Network Infrastructure by implementing firewalls, intrusion detection systems, and encryption protocols to protect the department's network. Regularly monitor network traffic for unusual activities are necessary.

In addition, there are some key actions that are necessary to assure a good cybersecurity in the departments:

- **Data Encryption**: Encrypt sensitive data both at rest and in transit to prevent unauthorised access in case of a breach.
- **Incident Response Plan**: Develop a clear and tested incident response plan to handle cybersecurity incidents effectively. This includes steps for containment, investigation, recovery, and communication.
- **Regular Security Audits and Assessments**: Conduct periodic security audits and assessments to evaluate the effectiveness of existing security measures and identify areas for improvement.
- **Vendor and Third-Party Risk Management**: Assess the cybersecurity measures of third-party vendors and contractors. Ensure that they comply with your department's security standards.

- **Continuous Monitoring and Improvement**: Implement systems for continuous monitoring of cybersecurity measures. Stay updated on emerging threats and adapt security strategies accordingly.

Revision #1
Created 9 July 2025 21:45:29 by RISA
Updated 9 July 2025 21:45:47 by RISA