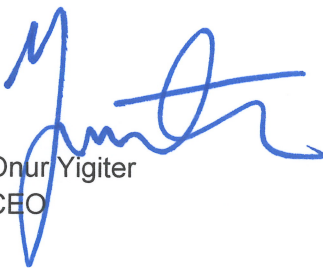


INFORMATION SECURITY POLICY

AMSTEEL considers that the information security is becoming more important as the technology develops and changes rapidly. **AMSTEEL** aims to ensure that all information technology users within the domain or its networks comply with rules related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority. This will be achieved through;

- Commitment to establish, apply and maintain information security procedure to manage the security of **AMSTEEL** information,
- Ensuring that **AMSTEEL** network system is designed, operated and maintained to minimize security threats and risks,
- Performing continual risk assessments and monitoring the security status of **AMSTEEL** network system to reduce the risks to ALARP (As Low As Reasonably Practicable), such risks will then be deemed as acceptable risks,
- Implementing effective information management systems and resourcing of required security arrangements that are subject to regular penetration tests and periodic updates,
- Implementing "Disaster Recovery Center" and "Contingency Plan" against system crash, cyberattack or hardware/software/network failures considering back up management and alternative network system to run the network system continuously.
- Providing an environment for transparent and effective information used and shared for reporting and analyzing security incidents as well as for sharing best practices,
- Ensuring that **AMSTEEL** employees receive regular training and information against information security threats and develop information security awareness, safe behavior and responsible attitude in **AMSTEEL** facilities.



Onur Yigiter
CEO

