SNF
WATER SCIENCE

DIGITAL SECURITY POLICY

This digital security policy outlines the measures and guidelines specific to SNF to protect digital assets and information. It is designed to minimize the risk of unauthorized access, data breaches, and other cyber threats. All SNF employees, contractors, and third-party vendors must adhere to this policy.

SNF guidelines are based on IT standards and best practices for data confidentiality, integrity, and availability. These standards include NIST, ISO27002, or ITIL frameworks.

Through its Security Operations Center, SNF monitors all security-related events across the Group to detect and respond to incidents and guarantee its subsidiaries the same level of knowledge, awareness, and protection.

SNF Policy key points are:

Access Control

- **User Authentication:** All users within SNF must have unique login credentials, including strong passwords and multi-factor authentication where possible.
- **Access Privileges:** SNF's digital assets and information should be granted based on the principle of least privilege, ensuring that employees only have access to the resources necessary for their role.
- **Account Management:** User accounts should be promptly disabled or removed upon termination or change in roles and responsibilities within SNF.

Data Protection

- **Data Monitoring:** All digital assets and information within SNF should be audited and monitored to prevent data exfiltration or misusage of sensitive data.
- **Encryption:** Sensitive data within SNF should be encrypted in transit and at rest using industry-standard encryption algorithms.
- **Data Backup:** Regular backups of critical data should be performed within SNF and stored securely offsite to ensure data recovery in case of a system failure or data loss.

Auditability

- Events occurring on the IT system must be monitored and stored with an appropriate retention period.
- Digital assets should be inventoried and managed by technologies allowing regular automated audits.

Network Security

- **Firewalls:** Network perimeters within SNF should be protected by firewalls to monitor and control incoming and outgoing traffic, preventing unauthorized access.
- **Intrusion Detection and Prevention Systems:** SNF should have systems to detect and prevent unauthorized access attempts and suspicious activities within the network.
- **Wireless Network Security:** Wireless networks within SNF should be secured with strong encryption, unique passwords, and regular monitoring to prevent unauthorized access.

Malware Protection

- **Antivirus Software:** All devices and systems within SNF should have up-to-date antivirus software installed and regularly updated to detect and mitigate malware threats.
- **Software Patching:** All software and operating systems within SNF should be updated daily with the latest security patches to address vulnerabilities and protect against potential digital threats.

Incident Response

- **Incident Reporting:** All employees within SNF should promptly report any suspected or actual security incidents to the designated IT team or security officer.
- **Incident Response Plan:** SNF should have an incident response plan to outline the steps to be taken during a security incident, including containment, investigation, and recovery.
- **Forensic Investigation:** In the event of a security breach within SNF, a thorough forensic investigation should be conducted to determine the cause and extent of damage and prevent future incidents.

Training and Awareness

- **Security Awareness Training:** Regular training sessions should be conducted within SNF to educate employees on digital security best practices, phishing awareness, and safe online behavior.
- **Policy Review:** This digital security policy should be reviewed periodically within SNF to ensure its effectiveness and relevance to evolving digital threats.

Compliance

- **Legal and Regulatory Compliance:** All digital security practices within SNF should comply with applicable laws, regulations, and industry standards.
- **Third-party Vendors:** Before engaging in business relationships, third-party vendors associated with SNF should be assessed for their digital security practices and compliance.

Enforcement

Failure to comply with this digital security policy within SNF may result in disciplinary action, including termination of employment or contract. Non-compliance may also lead to legal consequences.

Policy Review

This policy will be reviewed annually or as deemed necessary within SNF to ensure its effectiveness and alignment with changing security needs and technologies.

By following this digital security policy, SNF aims to protect its digital assets, maintain the confidentiality, integrity, and availability of information, and safeguard against unauthorized access and digital threats. This policy serves as a foundation for SNF's commitment to digital security. It sets the expectations for all individuals associated with SNF to actively participate in maintaining a secure digital environment.

SNF WATER SCIENCE