Current Status and Strategies of Enterprise-wide Security Governance in Public Institutions

1. Introduction

Korea Environment Corporation (K-eco) was established to lead the transition toward a carbon-neutral society and to create a safe and sustainable living environment. With the acceleration of digital transformation, the importance of enterprise-wide security governance has grown significantly. Establishing a comprehensive security management system has become essential for ensuring organizational sustainability and maintaining public trust. This report summarizes the current status and strategies of public institutions' security governance, focusing on the case of K-eco.

---

2. Overview of K-eco

Since its establishment in 2010, K-eco has set strategic goals such as carbon neutrality, clean air, healthy water environments, circular economy, and safe living conditions. The organization consists of its headquarters and eight regional environmental divisions, with over 3,000 employees. The Digital Innovation Office is responsible for information security and personal data protection, serving as the central unit for governance.

---

3. Security Governance System

3.1 Governance Structure

- The **National Intelligence Service (NIS)** oversees national information security policy, while the **Ministry of Environment** supervises implementation.
- K-eco's Chairman delegates responsibilities to the **Chief Information Security Officer (CISO)** and the Director of the Digital Innovation Office, supported by departmental security officers.
- The **Information Security Review Committee** handles regulatory improvements, incident management, and policy violations to ensure effective operations.

3.2 Core Security Activities

- Establishment and enforcement of information security and data protection policies
- Technical measures such as network segregation, VPN/VDI operations, and media control
- Compliance with NIS and Personal Information Protection Commission (PIPC) evaluations
- Continuous monitoring and internal audits through the Security Operations Center (SOC)

---

4. Information Security Practices

- **Commemorative Days:** Campaigns and joint activities during the national “Information Security Day” and “Personal Information Protection Day” to raise awareness through training and phishing simulations.
- **Organization-wide Engagement:** Activities such as the “Security Golden Bell” quiz and “Security 365” campaign foster daily awareness.
- **Leadership-driven Efforts:** The CEO leads security declaration ceremonies, while the CISO provides training at overseas offices and participates in security forums.
- **Technical Enhancements:** Initiatives include VDI for server administrators, strengthened access controls, port scanning, EDR deployment, and compliance with national cloud security guidelines.

---

5. Evaluation Strategies

5.1 Preparation

- Regular training and knowledge retention assessments
- Briefings on evaluation indicators and evidence documentation methods
- Analysis of changes in evaluation metrics and focused improvements

5.2 On-site Assessments

- Preparation of evidence in PDF/Excel format for readability
- Technical inspections such as port scanning and continuous asset updates
- Immediate responses and clarifications during inspection sessions

5.3 Response to Evaluation Indicators

- **Human Resources (10201):** Proper recognition and allocation of personal data protection staff
- **Budget (10501):** Independent allocation and management of security budgets
- **Vendor Training (10901):** Verification of contractor participation in security education
- **Executive Reporting (11601):** Strengthened reporting to the CEO and senior executives
- **System Operation (20102):** Pre-checking vulnerabilities in inter-network transfer systems
- **Access Control (20501):** Preventing exposure of administrator login pages
- **Log Management (30401):** Maintaining access logs for at least one year
- **Data Encryption (30501):** Ensuring proper use of encryption algorithms (AES, ARIA, DES)
- **DB Access Control (30502):** Applying firewall rules or specialized DB security solutions to track logs

---

6. Future Directions

Public institutions must expand security governance beyond regulatory compliance, positioning it as a foundation for management innovation and ESG practices. K-eco should strengthen its strategy in the following areas:

1. **Risk-based Management:** Integrated management of information security and privacy risks
2. **Leadership Engagement:** Enhanced decision-making roles for CEOs and CISOs in governance
3. **Technology-driven Security:** Expanded adoption of cloud, big data, and AI-based security solutions
4. **Collaborative Networks:** Stronger coordination with NIS, Ministry of Environment, and peer institutions
5. **Cultural Expansion:** Continuous awareness campaigns and embedding security into organizational culture

---

7. Conclusion

Enterprise-wide security governance in public institutions must evolve into a holistic system that involves all organizational levels. The case of K-eco demonstrates an integrated approach combining policy, technology, leadership, cultural engagement, and compliance evaluations. Strengthening these strategies will enable public institutions to achieve both secure digital transformation and ESG management goals, contributing to long-term sustainability and public trust.