IT GENERAL CONTROLS (ITGC)

AND

IT APPLICATION CONTROLS (ITAC)

POLICY AND PROCEDURES

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

---

Executive Summary

The North South Power Company Limited (NSPCL) ITGC and ITAC Policy provides a comprehensive framework to ensure the security, integrity, and effective management of the company's IT systems and applications. Building on existing policies such as user account management, change management, data backup, physical security, and software development, establishes robust controls around access management, change procedures, data protection, physical safeguards, and application security. This integrated approach aims to mitigate risks, ensure regulatory compliance, and support operational efficiency by implementing systematic, best-practice controls that safeguard data integrity, confidentiality, and system availability, while promoting a culture of continuous improvement and risk mitigation across the organization.

Table of Contents

Commented [OA1]: Format for structure

1. Purpose

This policy establishes NSPCL's commitment to implementing and maintaining a comprehensive framework of IT General Controls (ITGC) and IT Application Controls (ITAC) to safeguard the confidentiality, integrity, and availability of its information systems and data. It mandates adherence to relevant organizational policies and industry best practices, including controls around access management, change processes, data security, physical safeguards, and secure application development. Through disciplined implementation, regular review, and continuous improvement of these controls, NSPCL aims to mitigate risks, protect its assets, and ensure operational resilience across all IT functions and systems.

2. Scope

This policy applies to all information technology systems, applications, data, and personnel involved in managing and operating NSPCL's IT infrastructure.

Part I: IT General Controls (ITGC)

3. User Account Management

Objective: To ensure user access is appropriately provisioned, managed, and revoked, minimizing unauthorized access.

Controls:

- **Access Provisioning:** Follow the existing NSPCL User Account Management Policy and ERP User Access Policy, ensuring access is granted based on role, necessity, and approval.
- **Role-Based Access Control (RBAC):** Implement role-based access controls aligned with the RBAC Policy to assign permissions based on job responsibilities.
- **Account Review:** Conduct periodic reviews (bi-annually) of user accounts to verify access appropriateness.
- **Account Termination:** Remove or disable access immediately upon employee departure or role change, in accordance with the User Account Management Procedure.

Commented [OA2]: ERP User Access Rights & Review Policy

4. Change Management

Objective: To manage changes in IT systems with minimal risk and disruption.

Controls:

- Adhere to NSPCL Change Management Policy and Procedure.
- All changes must be documented, reviewed, tested, and approved before implementation.
- Emergency changes must follow predefined procedures, with post-implementation reviews.
- Maintain records of change activities for audit purposes.

5. Data Backup and Recovery

Objective: To ensure critical data is backed up regularly and recoverable in case of loss.

Controls:

- Follow NSPCL Backup Usage Policy and Data Backup and Recovery Policy.
- Schedule daily backups of critical systems and data.
- Test backup restorations periodically to verify integrity and recoverability.
- Maintain secure storage of backup copies, including off-site backups as per Data Migration Policy.

6. Physical and Environmental Security

Objective: To safeguard physical access to IT infrastructure.

Controls:

- Implement physical access controls compliant with NSPCL Physical Security and Access Control Policy.
- Monitor access points with logs and surveillance.
- Protect data centers and server rooms from environmental hazards per policy guidelines.

Commented [OA3]: This policy is not provided in the folder

Commented [OA4]: This is also not provided in the folder, would it be right to assume they are pre-existing policies

Commented [OA5]: Same as above

7. Application Development and Maintenance

Objective: To ensure software is developed, acquired, and maintained securely and effectively.

Controls:

- Follow NSPCL Software Development, Acquisition, and Maintenance Policy.
- Conduct security testing during software development phases.
- Use standardized procedures for software updates and patches.
- Document all software changes and maintain version control.

Part II: IT Application Controls (ITAC)

8. Access Controls

- **Segregation of Duties:** Enforce role separation to prevent conflicts of interest.
- **User Authentication:** Implement multi-factor authentication where feasible.
- **Authorization:** Ensure system permissions align with user roles and are reviewed regularly.

9. Data Integrity and Validation

- Validate data inputs at the application level to prevent errors and fraud.
- Use application controls such as automatic calculations, audit trails, and validation routines.

10. Data Privacy and Protection

- Implement encryption for sensitive data at rest and in transit, following Data Privacy and Protection Policy.
- Restrict access to sensitive data based on the principle of least privilege.
- Monitor and log access to critical systems and data.

11. Change Controls for Applications

- Apply controlled change procedures for software updates.
- Maintain documentation of all modifications, including testing and approval.

12. Incident Management

- Establish and follow incident response procedures for security breaches.
- Log, assess, and respond to security incidents promptly.

Commented [OA6]: same as above

13. Review and Revision

This policy will undergo a formal review every two (2) years to ensure its continued relevance and effectiveness. The review will be conducted by the IT Security Team in collaboration with key stakeholders. If significant changes in technology, regulatory requirements, or threat landscape arise before the next scheduled review, an addendum will be issued and attached as an update to relevant sections of the policy. Such interim updates will remain in effect until the next comprehensive review and integration into the core policy.