Information Technology Policy for Kalinga Vysya Samaj, NCR Delhi

1. Purpose

This policy outlines the guidelines and responsibilities for the use, management, and security of Information Technology (IT) resources owned by Kalinga Vysya Samaj, NCR Delhi (hereafter referred to as "the Samaj"). It aims to ensure the integrity, confidentiality, and availability of the Samaj's IT assets.

2. Scope

This policy applies to all members, employees, volunteers, contractors, and third parties who access or use the Samaj's IT resources, including but not limited to:

- Website Domain: www.kalingavysyasamaj.com (Managed by Boyina Web - Mr. Srinivas Boyina – 9899988749 / 8802533739)
- Email domain: kalingavysyasamaj@gmail.com (Managed by Mr. Ashok Boyina – 9312210058)
- Mobile applications: Kalinga Vysya Samaj Delhi & NCR Mobile App made by Javin (Managed by Javin Infosystems - Mr. Deepak Jain – 7838408888)
- Hardware and software systems and licenses: As and when procured (As on 1st March 2025 we have made no investment on these)
- Network infrastructure: As and when procured (As on 1st March 2025 we have made no investment on these)

3. Ownership and Management of IT Assets

- All IT assets are the exclusive property of the Samaj
- The President holds ultimate responsibility for all IT credentials and will disseminate access to authorized individuals on a need-to-know basis.
- A designated IT Administrator, appointed by the President, will manage day-to-day IT operations and ensure compliance with this policy.

4. Acceptable Use

Users of the Samaj's IT resources must:

- Use IT assets solely for activities aligned with the Samaj's mission and objectives.
- Protect login credentials and refrain from sharing them without proper authorization.
- Report any security incidents or breaches immediately to the IT Administrator.

Users must not:

- Engage in activities that could harm the Samaj's reputation or operations.
- Access, download, or distribute inappropriate or unauthorized content.
- Install unapproved software or make unauthorized changes to IT systems.

5. Security Measures

- Regularly update passwords and use strong, unique combinations.

- Implement antivirus and anti-malware solutions on all devices accessing the Samaj's network.
- Conduct periodic security audits and vulnerability assessments to identify and mitigate risks.

6. Data Protection and Privacy

- Collect, store, and process personal data in compliance with applicable laws and regulations.
- Restrict access to sensitive information to authorized personnel only.
- Ensure secure backup of critical data and establish disaster recovery plans.

7. Incident Response

- Establish an incident response plan detailing procedures for various security events.
- Train relevant personnel on incident identification, reporting, and mitigation.
- Document all incidents and responses to prevent future occurrences.

8. IT Asset Inventory

Maintain a comprehensive inventory of all IT assets, including:

- Hardware: Computers, servers, networking equipment, mobile devices.
- Software: Licensed applications, operating systems.
- Digital Assets: Domain names, SSL certificates, social media accounts.

9. Credential Management

- The President retains master credentials for all IT assets.
- Authorized users will receive access credentials based on their roles and responsibilities.
- Regularly review and update access permissions to reflect current organizational needs.

10. Policy Compliance

- Non-compliance with this policy may result in disciplinary action, including revocation of access privileges or legal proceedings.
- Regularly review and update this policy to adapt to evolving technological and organizational changes.

11. Policy Review

This policy will be reviewed annually or as required to ensure its relevance and effectiveness in addressing the Samaj's IT governance needs.

*****