DEVELOPMENT INITIATIVES BY SOCIAL ANIMATION (DISA)

POLICY ON INFORMATION TECHNOLOGY

1. Introduction

Development Initiatives By Social Animation (DISA) recognizes the importance of Information Technology (IT) in enhancing organizational efficiency, effectiveness, and transparency. This policy outlines the guidelines and procedures governing the use of IT resources to ensure compliance with Government regulations and promote responsible and secure IT practices.

2. Scope

This policy applies to all employees, volunteers, contractors, and third-party users who have access to DISA's IT resources, including hardware, software, networks, and data, across the places of Interventions and Programme Implementtion.

3. Objectives

- To protect the confidentiality, integrity, and availability of DISA's IT resources and data.
- To ensure compliance with relevant Government regulations, including data protection and privacy laws.
- To promote responsible and ethical use of IT resources for organizational purposes.
- To mitigate risks associated with cyber security threats, data breaches, and unauthorized access.
- To facilitate the effective and efficient utilization of IT resources to support DISA's mission and objectives.

4. Acceptable Use of IT Resources

- IT resources provided by DISA are to be used solely for legitimate organizational purposes.
- Users must adhere to all applicable laws, regulations, and organizational policies when using IT resources.
- Prohibited activities include but are not limited to:

✓ Unauthorized access to or use of IT systems or data.
✓ Distribution of malicious software or engaging in hacking or phishing activities.
✓ Violation of copyright or intellectual property rights.
✓ Use of IT resources for personal gain or illegal activities.

5. Data Security and Privacy

- Users must protect sensitive and confidential data entrusted to DISA from unauthorized access, disclosure, or modification.
- Data encryption, access controls, and password protection mechanisms shall be implemented to safeguard data integrity and privacy.
- Personal data shall be collected, processed, and stored in accordance with applicable data protection laws and privacy regulations.

6. Cyber Security Measures

- DISA shall implement technical and organizational measures to prevent, detect, and respond to cyber security threats, including malware, phishing attacks, and unauthorized access.
- Regular security assessments, audits, and penetration testing shall be conducted **to identify and mitigate vulnerabilities in IT systems and networks.**

7. Use of Personal Devices and BYOD (Bring Your Own Device)

- Personal devices may be permitted for work-related purposes subject to approval and compliance with DISA's IT policies and security standards.
- BYOD users shall adhere to additional security measures, such as device encryption, remote wipe capabilities, and installation of security software.

8. Software and Hardware Acquisition

- All software and hardware acquisitions shall be authorized and procured through official channels in compliance with procurement policies and budgetary constraints.
- Users shall use licensed software and ensure compliance with software vendor agreements and copyright laws.

9. Reporting Security Incidents and Policy Violations

- Users shall promptly report any suspected security incidents, data breaches, or policy violations to the designated IT Personnel or Security Officer.
- DISA shall investigate reported incidents and take appropriate remedial actions to mitigate risks and prevent recurrence.

10. Training and Awareness

- DISA shall provide regular training and awareness programs to educate users about IT security best practices, policies, and procedures.
- Users shall receive training on how to recognize and respond to cybersecurity threats, phishing emails, and social engineering attacks.

11. Compliance and Enforcement

- Compliance with this policy shall be monitored through regular audits, assessments, and reviews.
- Non-compliance with this policy may result in disciplinary action, including revocation of IT privileges, termination of employment, or legal consequences.

12. Policy Review and Updates

- This policy shall be reviewed periodically to ensure alignment with evolving government regulations, industry standards, and best practices.
- Updates to the policy shall be communicated to all stakeholders to ensure awareness and compliance.

13. Conclusion

DISA is committed to maintaining a secure, reliable, and ethical IT environment to support its mission and operations effectively. This policy serves as a framework for promoting responsible IT practices and ensuring the protection of organizational assets and data.

Secretary
Development Initiatives by Social Animation (DISA)