ISO / IEC 27001:2022 Lead Implementer Course

Exercise 6:

- Write your Information Security Policy
- Considering your company as a case study for ISO 27001:2022 implementation
- Take a blank piece of a white paper, write (by-hand). Do not copy or review; trust your memory.
- Take a clear snapshot of the paper, create a folder on Google Drive 'ISO 27001:2022 Lead' and save the snapshot (If you did not create in Exercise A)
- Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
- Facebook link: facebook.com/profile.php?id=61556175711538\

Follow me on my social media platforms to learn more about ISO / IEC 27001:2022 via my posts:

- LinkedIn: linkedin.com/in/john-kimani-13831329b
- Facebook: facebook.com/profile.php?id=61556175711538
- Quora: quora.com/profile/The-Cyber-Hackers-Diary
- Pinterest: pinterest.com/hackersdiary
- YouTube: www.youtube.com/@CyberHackersDiary

Information Security Policy.
Stoopid Boy Animations Inc.

1. Introduction:-

Stoopid Boy Animations Inc. is committed to safeguarding confidentiality, integrity, and availability of all physical and electronic assets to ensure business continuity, minimize business damage, and maximize opportunities. This policy outlines our commitment to information security in compliance with ISO 27001:2022 standards.

2. Purpose:-

The purpose of this Information Security Policy is to ensure that all information and information used in Stoopid Animations Inc. are adequately protected from risks such as unauthorized access, use, disclosure, disruption, modification or destruction. This policy is designed to protect information assets and manage information security risks effectively.

3. Scope:-

This policy applies to all employees, contractors, consultants, temporary staff, and any other workers at Stoopid Boy Animations Inc. including all personnel affiliated with third parties. It encompasses all information assets owned or leased by Stoopid Boy Animations Inc.

4 Information Security Objectives:-

- Protect the confidentiality, integrity and availability of information
- Comply with relevant legal, regulatory and contractual requirements
- Ensure all employees are aware of and understand their responsibilities regarding information security.
- Provide a safe and secure working environment.
- Implement and maintain effective incident management procedures.

5. Governance and Responsibility:-

- Chief Information Security Officer (CISO):- Responsible for developing, implementing and maintaining the information Security program.
- Management:- Ensure that information policies and practices are enforced
- Employees:- Follow information Security policies and report any security incidents or Vulnerabilities.

6. Risk Management:-

A systematic risk management process shall be conducted to identify assess, and manage risks to the Organization's information assets. This include regular risk assessments, implementing appropriate risk mitigation controls, and monitoring the effectiveness of these controls.

7 Asset Management:-

All information assets shall be identified, classified, and managed according to their Sensitivity and Criticality. An inventory of information assets shall be maintained regularly.

8 Access Control:-

Access to information and information systems shall be granted on a need-to-know basis, aligned with job responsibility. Strong authentication mechanisms shall be used to verify the identity of users accessing information systems.

9. Physical and Environmental Security.

Physical security measure shall be implemented and documented to ensure the secure and reliable operation of information processing facilities. This incude change management, Capacity management and

10. Operations Security:-
Operations procedures and responsibilities shall be documented and implemented to ensure secure and reliable operation of information processing facilities. This includes change management, capacity management and malware protection.

11. Communications Security:-
Measures shall be in place to protect the information in networks and the supporting infrastructure. This includes securing network devices, protecting data during transmission, and ensuring the secure configuration of network devices.

12. Incident Management:-
An incident management process shall be established to ensure effective and timely response to information security incidents. All incidents must be reported immediately to the designated incident response team.

13. Business Continuity Management:-
Business Continuity plans shall be developed implemented, and tested regularly to ensure that the Organization can continue its critical operations during and after a disruptive incident.

14. Compliance:-
Stoopid Boy Animations Inc. shall comply with relevant laws, regulations, and contractual obligations. Regular audits and reviews shall be conducted to ensure compliance with the information security policy and procedures.

15. Continuous Improvement:-
The information security management system (ISMS) shall be continuously improved by regularly reviewing the policy, objectives,

16 Policy Review:-

This Information Security Policy shall be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness.

17 Approval:-

This policy has been approved by the executive management and is supported by all levels of management within Stoopid Boy Animations Inc.

Approved by:-

JOHN KIMANI MUNGAI

Regulatory Compliance Officer.

Stoopid Boy Animations Inc.