ISO / IEC 27001:2022 Lead Implementer Course

Exercise 18:

Instructions:

- Create a communication plan
- 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

@ The Cyber Hacker's Diary

Communication Plan for ISMS

Stoopid Boy Animations Inc.

ISO/IEC 27001:2022 Implementation

Purpose:-

To establish a structured approach for internal and external communication regarding Information Security Management Systems (ISMS) implementation and maintenance

Scope:-

This communication plan applies to all stakeholders of Stoopid Boy Animations Inc., including employees, management, and external parties.

Objectives:-

- Ensure clear and consistent communication about ISMS policies, procedures, and updates.
- Facilitate awareness and understanding of information security responsibilities.
- Promote a culture of security within the Organization.

Stakeholders:-

- **Internal:-** Employees, IT Department, Management, Information Security Management
- **External:-** Clients, Suppliers, Regulatory Bodies, Auditors.

Communication Methods:-

- **Email:-** For formal communication, policy updates, and incident notifications
- **Meetings:-** Regular meetings for discussing ISMS status, changes & feedback
- **Intranet:-** Centralized repository for ISMS documents, policies & training materials
- **Training Sessions:-** Scheduled sessions for educating employees on ISMS practices and responsibilities.

Frequency :-

- Daily :- Incident reporting and critical updates
- Weekly :- Team meetings to discuss ongoing ISMS activities
- Monthly :- Management reports and newsletters
- Quarterly :- Training sessions and comprehensive ISMS status
- Annually :- Review and update of ISMS policies & proce

Responsibilities :-

① Information Security Manager :-
Oversee communication plan execution, review and approve messages, coordinate with departments.

② IT Department :-
Provide technical support for Communication channels, ensure information security for communication tools.

③ Department Heads :-
Ensure dissemination of ISMS information within their teams, provide feedback to the Information Security Manager.

Evaluation :-

① Feedback Surveys :-
Collect feedback from employees and stakeholders on the effectiveness of Communication.

② Review Meetings :-
Regularly assess the Communication plan's effectiveness and make necessary adjustments.

Confidentiality :-
Ensure all Communication is classified according to the Organization's information classification policy and handled accordingly to maintain Confidentiality & integrity.