ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

SELF ASSESSMENT QUESTIONNAIRE

FOR GAP ANALYSIS

SELF ASSESSMENT QUESTIONNAIRE

FOR GAP ANALYSIS

THE SELF ASSESSMENT TOOL (THE "ASSESSMENT") YOU ARE ABOUT TO PROCEED WITH IS BASED UPON THE INFORMATION YOU SUBMIT AND IS THEREFORE YOUR OWN ANALYSIS. THE INFORMATION CONTAINED IN THIS ASSESSMENT IS FOR YOUR PERSONAL USE ONLY. THE OUTCOME FROM THIS ASSESSMENT IS NOT IN ANY WAY ENDORSED, CHECKED OR APPROVED.

EDIT OR DOWNLOAD THIS PRINTABLE ONLINE QUESTIONNAIRE.

BUSINESS DETAILS

CONTACT NAME

COMPANY NAME

EMAIL

COMPANY EMAIL

CONTACT NUMBER:

MARK ✓ FOR YES OR LEAVE BLANK FOR NO

THE ORGANIZATION AND IT'S CONTENTS:

1.) HAVE THE INTERNAL AND EXTERNAL ISSUES, AND THE REQUIREMENTS OF INTERESTED PARTIES RELATED TO ISMS ACHIEVED IT'S OUTCOMES, BEEN DETERMINED? ☐

2.) ARE ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES BEEN PLANNED? ☐

3.) HAS INTEGRATATION INTO THE ISMS PROCESSES EVALUATED FOR EFFECTIVENESS? ☐

4.) DO YOU HAVE DOCUMENTS THAT ESTABLISH RISK PROCESS ASSESSMENTS AND PERFORMANCE RESULTS, INCLUDING A RISK ACCEPTANCE CRITERIA? ☐

RISK ASSESSEMENT PROCESS:

5.) HAVE YOU PERFORMED THE FOLLOWING:

- IDENTIFY INFORMATION SECURITY RISKS THAT ARE ASSOCIATED WITH THE LOSS OF CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF INFORMATION
- ANALYSE INFORMATION SECURITY RISKS WHICH HAVE TAKEN LIKELIHOOD AND CONSEQUENCE INTO CONSIDERATION
- EVALUATE INFORMATION SECURITY RISKS AND ALSO COMPARE THE RESULTS OF SUCH RISKS WITH THE ESTABLISHED RISK CRITERIA ☐

6.) DO YOU HAVE AN ESTABLISHED RISK TREATMENT PLAN (WITH CONTROLS SELECTED FROM ISO/IEC 27001 ANNEX A CONTROLS) THAT ADDRESSES ALL RISKS THAT ARE IDENTIFIED? ☐

7.) DO YOU HAVE AN ESTABLSIHED STATEMENT OF APPLICABLITY (SOA) ☐

8.) HAVE MEASURABLE ISMS OBJECTIVES AND TARGETS BEEN ESTABLISHED, DOCUMENTED AND COMMUNICATED THROUGHOUT THE ORGANIZATION? ☐

9.) ARE THESE POLICIES BEING REGULARLY REVIEWED? ☐

10.) IN SETTING ITS OBJECTIVES, HAS THE ORGANIZATION DETERMINED WHAT NEEDS TO BE DONE, WHEN AND BY WHOM? ☐

11.) HAS A PROGRAMME TO ENSURE THE ISMS ACHIEVES ITS OUTCOMES, REQUIREMENTS AND OBJECTIVES BEEN DEVELOPED AND IMPLEMENTED? ☐

12.) HAS A PROGRAMME TO ENSURE THE ISMS ACHIEVES ITS OUTCOMES, REQUIREMENTS AND OBJECTIVES BEEN DEVELOPED AND IMPLEMENTED? ☐

13.) IS DOCUMENTED EVIDENCE RETAINED TO DEMONSTRATE THAT PROCESSES HAVE BEEN CARRIED OUT AS PLANNED? ☐

14.) ARE CHANGES PLANNED AND CONTROLLED, AND UNINTENDED CHANGES REVIEWED TO MITIGATE ANY ADVERSE RESULTS? ☐

15.) HAVE OUTSOURCED PROCESSES BEEN DETERMINED AND ARE THEY CONTROLLED? ☐

18.) ARE INFORMATION SECURITY RISK ASSESSMENTS PERFORMED AT PLANNED INTERVALS OR WHEN SIGNIFICANT CHANGES OCCUR, AND IS DOCUMENTED INFORMATION RETAINED? ☐

19.) HAS THE INFORMATION SECURITY RISK TREATMENT PLAN BEEN IMPLEMENTED AND DOCUMENTED INFORMATION RETAINED? ☐

20.) ARE THESE POLICIES BEING REGULARLY REVIEWED? ☐

SECURITY CONTROLS:

21.) HAS A MANAGEMENT FRAMEWORK BEEN ESTABLISHED TO CONTROL THE IMPLEMENTATION AND OPERATION OF SECURITY WITHIN THE ORGANIZATION, INCLUDING ASSIGNMENT OF RESPONSIBILITIES AND SEGREGATION OF CONFLICTING DUTIES? ☐

22.) ARE APPROPRIATE CONTACTS WITH AUTHORITIES AND SPECIAL INTEREST GROUPS MAINTAINED? ☐

23.) IS THERE A POLICY, PROCEDURE OR PROCESS FOR INFORMATION SECURITY ADDRESSED IN PROJECTS? ☐

24.) IS THERE A MOBILE DEVICE POLICY OR PROCEDURE IN PLACE? ☐

25.) IS THERE A TELEWORKING POLICY OR GUIDELINE IN PLACE? ☐

26.) ARE HUMAN RESOURCES SUBJECT TO SCREENING BEFORE THEY JOIN THE ORGANIZATION? ☐

27.) DO THEY HAVE TERMS AND CONDITIONS OF EMPLOYMENT DEFINING THEIR INFORMATION SECURITY RESPONSIBILITIES? ☐

28.) ARE EMPLOYEES REQUIRED TO ADHERE TO THE INFORMATION SECURITY POLICIES AND PROCEDURES? ☐

29.) ARE EMPLOYEES PROVIDED WITH AWARENESS, EDUCATION AND TRAINING? ☐

30.) IS THERE A DISCIPLINARY PROCESS WHEN EMPLOYEES VIOLATES THE COMPANY POLICIES LIKE THE INFORMATION SECURITY POLICIES? ☐

31.) ARE THE INFORMATION SECURITY RESPONSIBILITIES AND DUTIES COMMUNICATED AND ENFORCED FOR EMPLOYEES WHO TERMINATE OR CHANGE EMPLOYMENT? ☐

32.) IS THERE AN INVENTORY OF ASSETS ASSOCIATED WITH INFORMATION AND INFORMATION PROCESSING, HAVE OWNERS BEEN ASSIGNED? ☐

33.) ARE RULES FOR ACCEPTABLE USE OF ASSETS DEFINED? ☐

34.) ARE RULES FOR RETURN OF ASSETS DEFINED? ☐

35.) IS THERE AN INFORMATION CLASSIFICATION POLICY AND THE INFORMATION IS CLASSIFIED IN ACCORDANCE WITH THIS POLICY ☐

36.) IS INFORMATION APPROPRIATELY LABELLED IN ACCORDANCE WITH THE INFORMATION CLASSIFICATION POLICY? ☐

37.) ARE THERE PROCEDURES FOR:

- TRANSIT OF MEDIA CONTAINING INFORMATION? ☐
- THE MANAGEMENT OF MEDIA CONTAINING INFORMATION? ☐
- THE REMOVAL, DISPOSAL OF MEDIA CONTAINING INFORMATION? ☐
- HAS AN ACCESS CONTROL POLICY BEEN DEFINED AND REVIEWED? ☐

38.) IS USER ACCESS TO THE NETWORK CONTROLLED IN LINE WITH THE POLICY? ☐

39.) IS THERE A FORMAL USER REGISTRATION PROCESS ASSIGNING AND REVOKING ACCESS AND ACCESS RIGHTS TO SYSTEMS AND SERVICES? ☐

40.) ARE PRIVILEGED ACCESS RIGHTS RESTRICTED AND CONTROLLED? ☐

41.) IS SECRET AUTHENTICATION INFORMATION CONTROLLED, AND USERS ARE MADE AWARE OF THE PRACTICES FOR USE? ☐

42.) IS ACCESS TO INFORMATION RESTRICTED IN LINE WITH THE ACCESS CONTROL POLICY, AND IS ACCESS CONTROLLED VIA A SECURE LOG-ON PROCEDURE? ☐

43.) ARE PASSWORD MANAGEMENT SYSTEMS INTERACTIVE AND DO THEY ENFORCE A QUALITY PASSWORD? ☐

44.) IS THE USE OF UTILITY PROGRAMS AND ACCESS TO PROGRAM SOURCE CODE RESTRICTED? ☐

45.) ARE RULES FOR ACCEPTABLE USE OF ASSETS DEFINED ☐

46.) ARE RULES FOR RETURN OF ASSETS DEFINED? ☐

47.) IS THERE AN INFORMATION CLASSIFICATION POLICY AND THE INFORMATION IS CLASSIFIED IN ACCORDANCE WITH THIS POLICY ☐

48.) IS INFORMATION APPROPRIATELY LABELLED IN ACCORDANCE WITH THE INFORMATION CLASSIFICATION POLICY? ☐

49.) ARE THERE PROCEDURES FOR TRANSIT OF MEDIA CONTAINING INFORMATION? ☐

50.) ARE THERE PROCEDURES FOR THE MANAGEMENT OF MEDIA CONTAINING INFORMATION? ☐

51.) ARE THERE PROCEDURES FOR THE REMOVAL, DISPOSAL OF MEDIA CONTAINING INFORMATION? ☐

52.) HAS AN ACCESS CONTROL POLICY BEEN DEFINED AND REVIEWED? ☐

53.) IS USER ACCESS TO THE NETWORK CONTROLLED IN LINE WITH THE POLICY? ☐

54.) IS THERE A FORMAL USER REGISTRATION PROCESS ASSIGNING AND REVOKING ACCESS AND ACCESS RIGHTS TO SYSTEMS AND SERVICES? ☐

55.) ARE PRIVILEGED ACCESS RIGHTS RESTRICTED AND CONTROLLED? ☐

56.) IS SECRET AUTHENTICATION INFORMATION CONTROLLED, AND USERS ARE MADE AWARE OF THE PRACTICES FOR USE? ☐

57.) IS ACCESS TO INFORMATION RESTRICTED IN LINE WITH THE ACCESS CONTROL POLICY, AND IS ACCESS CONTROLLED VIA A SECURE LOG-ON PROCEDURE? ☐

58.) ARE PASSWORD MANAGEMENT SYSTEMS INTERACTIVE AND DO THEY ENFORCE A QUALITY PASSWORD? ☐

59.) IS THE USE OF UTILITY PROGRAMS AND ACCESS TO PROGRAM SOURCE CODE RESTRICTED? ☐

60.) IS THERE A POLICY FOR THE USE OF CRYPTOGRAPHY? ☐

61.) IS THERE A POLICY, PROCEDURE OR GUIDELINE FOR THE USE OF KEY MANAGEMENT?	☐
62.) ARE THERE POLICIES AND CONTROLS TO PREVENT UNAUTHORISED PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES?	☐
63.) ARE THERE POLICIES AND CONTROLS TO PREVENT UNAUTHORISED PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES?	☐
64.) IS THERE A PROCEDURE OF WOKING IN SECURE AREA?	☐
65.) ARE THE EQUIPMENT AND ASSETS GIVEN PROPER SITING AND PROTECTION FROM ENVIRONMENT THREATS AND HAZARDS?	☐
66.) ARE ALL THESE EQUIPMENT AND ASSETS ADEQUATELY MAINTAINED?	☐
67.) IS THERE A DEFINED CLEAR DESK AND CLEAR SCREEN POLICY, PROCEDURE OR GUIDELINE?	☐
68.) DO YOU HAVE A THIRD PARTY (SUPPLIER, VENDOR) POLICY IN PLACE?	☐
69.) DO YOU HAVE AN INCIDENT RESPONSE PLAN?	☐
70.) DO YOU HAVE A BUSINESS CONTINUITY PLAN?	☐