|  |
| --- |
| **CYBERSECURITY MALAYSIA INFORMATION SECURITY MANAGEMENT SYSTEM**  **CERTIFICATION AND AUDIT SCHEME (CSM27001)** |

Please fill in the application form below to proceed with the CSM27001 application. Attach separate sheets if the space provided is insufficient. Supporting documents can be also attached.

CSM27001 Application Form for **MS ISO/IEC 27001:2013; or**

CSM27001 Application Form for **ISO/IEC 27001:2022**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **A: Organisation Information** | | | | | |
| 1. Registered organisation name | | | | | |
| 1. Company registration no. | |  | | | |
| 1. Business sector:   *(Kindly tick* √*)* | | Government  Banking & Finance  Information & Communications  Health Services  Emergency Services | | | Energy  Water  Transportation  Food & Agriculture  National Defence and Security  Others: *<Kindly indicate below>*  *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |
| 1. Legal status:   *(Kindly tick* √*)* | | Sdn Bhd/Private Limited  Berhad  Others <indicate below>  *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* | | | Bumiputera  Non bumiputera |
| 1. Corporate address | | Address: | | | |
| Postcode: | | | State: |
| 1. Authorised representative for CSM27001 ISMS details | | Name: | | | Tel No.: |
| Designation: | | | Email: |
| 1. Alternate contact details for the authorised representative | | Name: | | | Tel No.: |
| Designation: | | | Email: |
| 1. Corporate structure | | *<You may include as an attachment>* | | | |
| **B: ISMS Scope Description** | | | | | |
| 1. ISMS Scope Statement (kindly indicate exclusion (if any)) | |  | | | |
| 1. Description of the scope | |  | | | |
| 1. Justification for selecting the ISMS scope | |  | | | |
| 1. List all departments / units/ sections within ISMS scope | | |  |  |  | | --- | --- | --- | | Department/ unit/section | Activities/services | No of staff (including permanent / contract) | |  |  |  | |  |  |  | |  |  |  | | | | |
| 1. List services/ activities within ISMS scope which have been outsourced | |  | | | |
| C: Sites involved (within the ISMS scope) | | | | | |
| 1. Numbers of sites within ISMS scope \_\_\_\_\_\_\_\_\_\_\_   (including Data Centre and Disaster Recovery Site) | | | | | |
| Main Site | | | | | |
| 1. Address |  | | | | |
| 1. Services/Operations/ Activities within ISMS scope |  | | | | |
| 1. Depts Involved and Numbers of staff in each dept |  | | | | |
| 1. Official working hour / shift | *<Kindly indicate the number of shift and working hours, if applicable>* | | | | |
| Sites II (e.g. Data Centre) | | | | | |
| 1. Address |  | | | | |
| 1. Services/Operations/ Activities within ISMS scope |  | | | | |
| 1. Depts Involved and Numbers of staff in each dept |  | | | | |
| 1. Official working hour / shift | *<Kindly indicate the number of shift and working hours, if applicable>* | | | | |
| Sites III (e.g. Disaster Recovery Centre) | | | | | |
| 1. Address |  | | | | |
| 1. Services/Operations/ Activities within ISMS scope |  | | | | |
| 1. Depts Involved and Numbers of staff in each dept |  | | | | |
| 1. Official working hour / shift | *<Kindly indicate the number of shift and working hours, if applicable>* | | | | |
| D: Extent & diversity of technology utilized | | | | | |
| Information Systems/Applications | | | | | |
| 1. Numbers of Information Systems/Applications within ISMS Scope  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Name of Information Systems  /Applications | Function | Development or  Maintenance | In-house-Development / Off-the-shelf/ Outsourced | No of users | Type of users  *<Customers/*  *Third Party/ Staff/Super Admin/Others; Please specify>* | |  |  |  |  |  |  | |  |  |  |  |  |  | | | | | | |
| Networks & Encryption Technology | | | | | |
| |  |  |  |  | | --- | --- | --- | --- | | Networks  *Internet/Intranet/ Wireless/Others (Please specify)* | Function | Provide connection with encryption?  *<Please describe>* | Type of users  *< Staff/Contract staff/Visitor/Others; Please specify>* | |  |  |  |  | |  |  |  |  |   2. Encryption technology:  Sharing Documents *<Please describe>* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Emails *<Please describe>\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  Others *<Please describe> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* | | | | | |
| Servers | | | | | |
| 3. Numbers of Servers within ISMS Scope   |  |  |  | | --- | --- | --- | | Servers | Description | Operating Systems | |  |  |  | |  |  |  | |  |  |  | | | | | | |
| Other technology (please describe) | | | | | |
| *< Cloud Computing, SCADA, PCI-DSS, PA-DSS, IOT, Blockchain etc.>* | | | | | |
| **F. Legal, Regulatory and Contractual Aspects** | | | | | |
| 1. List all legal & regulatory compliance that the organisation must adhere to | | |  | | |
| **G.** **Management System Information** | | | | | |
| 1. Has your organisation been certified to other management system or adopt any management best practice? | | | | Yes  No  If Yes, please provide the name of the management system:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. Has your organization use a consultant for implementing the Information Security Management System (ISMS)? | | | | Yes  No  If Yes, please provide the name of the ISMS consultant:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­\_\_\_\_\_ | |
| 1. Please provide copy of the Statement of Applicability (SOA). | | | | Yes  No  If No, please provide expected completion date of the SOA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. Name of the methodology approaches of the Risk Assessment that being developed to your organization? | | | |  | |
| 1. Has the internal audit and management review been conducted? If yes, please provide the date.   Note: Certification audit can only be conducted upon completion of internal audit and management review. | | | | Internal audit date:  Yes. Date conducted: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  No. Targeted date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Management review date:  Yes. Date conducted: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  No. Targeted Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. When is your expected ISO/IEC 27001 certification date? <month/year> | | | | Targeted Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. Has CyberSecurity Malaysia provided any service to your organisation? | | | | Yes  No  If Yes, please provide the service name and month/year in which the service was completed:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. Access to organizational ISMS related information (such as ISMS records or information about design and effectiveness of controls) will be given during certification audit?   Note: CB will determine whether the ISMS can be adequately audited in the absence of such ISMS related information. If CB concludes that it is not possible to adequately audit the ISMS, CB will advise the that the certification audit cannot take place until appropriate access arrangements are granted. | | | | Yes  No  If No, please provide the ISMS related information that cannot be made available during certification audit:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

|  |  |  |
| --- | --- | --- |
| **For Internal Use Only** | Accept  Decline  (Justification for declining: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ) | Date Received: |
| CyberSecurity Malaysia’s Officer in Charge: |