Organization of Islamic Conference - Computer Emergency Response Team (OIC-CERT)

Membership Application Check List

(to be filled by the **applicant's sponsor**)

The list below provides a guideline for evaluating OIC-CERT Membership Application. The evaluation will be based on the relevancy of the prospective member's type of services provided, technical skills, contribution to the security community, expectation for joining as a member, ability to handle sensitive information, and CSIRT teams relationship track record.

1	**Relevancy of the Applicant's services to the security field** Services such as Incident Response Team, Information Security Consulting and Information Security Research Check all types of services and skills-set of the applicant to ensure the criteria of becoming an OIC-CERT member are suitable.	
2	**Contribution to the OIC-CERT community and the expectation of the Applicant.** * The Applicant's mission, focus, resources available for supporting the OIC-CERT activities and the Applicant's expectations as an OIC-CERT member are examined.	
	2.1 Check the Applicant's track record.	
	i.e. How often does the Applicant attend security related conferences?	
	i.e. How often does the Applicant give presentation at these conferences?	
	2.2 What is the Applicant contribution to the information security community?	
	2.2.1 writing papers	
	2.2.2 providing documentations	
	2.2.3 developing security tools	
	2.2.4 providing alerts and advisories	
	2.2.5 holding educational events, such as workshops, tutorials, conferences	

	2.2.6 active in information security mailing lists (please specify which mailing lists) ____ ____	
	2.3 Review the team’s expectations after joining as an OIC-CERT member.	
3	**Trust** * Clarify the Applicant’s policy with regards to the following:	
	3.1 Check the Applicant’s information security policy in handling sensitive information.	
	3.1.1 How is incoming information tagged or classified?	
	3.1.2 How is outgoing information tagged or classified?	
	3.1.3 What considerations are taken for disclosing sensitive information, especially incident related information exchanged with other teams?	
	3.1.4 Are there legal considerations taken into account with regards to information handling?	
	3.2 Check the track record of working relationship with other CERTs.	
	3.3 Check the Applicant’s policy in respect to:	
	3.3.1 Type of incidents and level of support	
	3.3.2 Co-operation, interaction and disclosure of information	
	3.3.3 Communication and authentication	