MEMBERSHIP APPLICATION

Organisation of Islamic Cooperation –
Computer Emergency Response Team (OIC-CERT)

1) MEMBERSHIP CATEGORY

The OIC-CERT is open to any suitable CERT / CSIRT and professionals that meet the criteria as stated in the following paragraphs.

The OIC-CERT has six types of memberships:

A) FULL Member

B) GENERAL Member

C) PROFESSIONAL Member

D) AFFILIATE Member

E) COMMERCIAL Member

F) FELLOWS Member

A) <u>FULL Member</u>

Requirements:

i) CERT or CSIRT or similar entity that is located and / or primarily functions within the jurisdiction of an OIC member countries.

ii) Not-for-profit and / or wholly or partially government funded.

iii) Authorized to represent the states interests.

iv) Application to be sponsored by one (1) OIC-CERT Full Member.

B) <u>GENERAL Member</u>

Requirements:

i) NGOs and Academia from an OIC member country that does not secure the authority of its host OIC member country, to represent the country’s interests.

ii) Application to be sponsored by one (1) OIC-CERT Full Member.

C) PROFESSIONAL Member

Requirements:

i) Individuals who have established their credibility and expertise in the information security areas.

ii) Application to be sponsored by one (1) OIC-CERT Full Member.

iii) An annual membership fee of USD50 will be imposed.

D) AFFILIATE Member

Requirements:

i) The membership is open to not-for-profit non-OIC institutions.

ii) Institutions from non-OIC member countries that is authorized to represent the countrys' cyber security interests.

iii) Application to be sponsored by two (2) OIC-CERT Full Members.

E) COMMERCIAL Member

Requirements:

i) Industrial / business organisation that deals with cyber security matters.

ii) Application to be sponsored by two (2) OIC-CERT Full Members.

iii) An annual membership fee of USD1000 will be imposed.

F) FELLOWS Member

Requirements:

i) Individuals co-founders of OIC-CERT and who use to actively represent their organization as OIC-CERT member for a minimum period of 5 years may apply for this membership. The application does not require any sponsorship by the OIC-CERT Full Members.

ii) Application will be discussed and subject to the approval of the OIC-CERT Board.

2) MEMBERSHIP APPLICATION PROCESS

i) Complete and submit the application form to the Secretariat.

ii) Upon receiving the application form, the Secretariat will check for the completeness of the details given.

iii) The completed application form will be reviewed and evaluated by the OIC-CERT Board.

iv) The applicants will be informed on the status of the application within 14 working days from acceptance of the application form.

MEMBERSHIP APPLICATION FORM

The Organisation of Islamic Cooperation-Computer Emergency Response Team (OIC-CERT)

APPLICATION FORM

Please complete the form and submit the application to OIC-CERT Secretariat at **secretariat@oic-cert.org**. The information provided will be treated as confidential. Only the Secretariat and the OIC-CERT Board will have the access to this information.

- **Membership type (Item 1)**
- **Official team name (Item2)**
- **Short Team name (Acronym)(Item 3)**
- **Team constituency (Item 8)**
- **Contact information (Item 12.1,12.2,12.3 and 12.4)**

1.	**Type of membership :**	
	i) FULL Member	
	ii) GENERAL Member	
	iii)PROFESSIONAL Member	
	iv)AFFILIATE Member	
	v) COMMERCIAL Member	
	vi) FELLOWS Member	
2	**Member Name**	
3	**Short Team Name (Acronym)** ***Note: NOT applicable for professional & fellows membership application***	
4	Host Organization and address	
5	Country located	
6	Establishment date	
7	Objective to join the OIC-CERT	

8	**Team Classifications (Check one or more) :** ***Note: NOT applicable for professional & fellows membership application***		
	i) Vendor Customer Base		
	ii) Internal to Host Organization		
	iii) ISP Customer Based		
	iv) Economy Based		
	v) University Based		
	vi) Other (please specify)		
9	Internet Domain Name		
10	Specify the constituency (Mandatory to attach letter of support from the authority which approved your application to join OIC-CERT.) ***Note: Applicable for FULL membership application only.***		
11	Please describe relevant technical and management skill-set for the membership category. ***Note: You may attach relevant documents to support this application.***		
12	**Contact Information (The information from 12.1 to 12.4 will be made public)**		
	12.1	Official Contact Number (all fields below are mandatory)	
		i) Time-zone (relative to GMT)	
		ii) Days/hours of Operation	
		iii) Name	
		iv) Designation	
		v) Contact Number	
		vi) Email Address	

	12.2	Emergency Contact Number (if different from the above “Regular Phone number”)	
		i) Time-zone (relative to GMT)	
		ii) Contact Number	
		iii) Days/hours of Operation	
		iv) Name	
		v) Designation	
		vi) Contact Number	
		vii) Email Address	
		viii) Fax Number (optional)	
	12.3	Website URL (optional)	
	12.4	OIC-CERT representative This person will be responsible for providing information to the sponsor and the OIC-CERT Secretariat when required during the membership application process. Once the application has been approved, this person will be responsible for keeping the teams contact information up to date and to represent its team during OIC-CERT general meetings.	
		i) Name of the person	
		ii) Designation	
		iii) Contact telephone number	
		iv) Email Address (mandatory) Recommendation: " oiccert-rep@your.domain "	
	12.5	Aliases to be included in OIC-CERT mailing list. OIC-CERT-TEAMS mailing list : " oiccert-team@your.domain " Recommendation " oiccert-team@your.domain "	
		Emails Address (mandatory)	

13	PGP/GPG Public Keys [Note: All submitted public keys must be self-signed, and signed by the applicant team's representative provided above]		
	13.1	PGP/GPG Public Key of the OIC-CERT -rep (mandatory)	
		User ID	
		Key ID	0x
		Key Type (bit)	
		Key Size	
		Expiration	
		Fingerprint	
	[Note: Please include public key block of representative here. The public key must be signed by the sponsor in addition to the requirements listed above. The key of the oiccert-rep should be a key of a person and not a "role key" only. (Mandatory)]		
	13.2	PGP/GPG Public Key for Team usage (mandatory)	
		User ID	
		Key ID	0x
		Key Type (bit)	
		Key Size	
		Expiration	
		Fingerprint	
	[Note: Please include public key block for team keys here.]		

	13.3	PGP/GPG Public Key of other team members (optional - please include an appropriate number of entries by cut and paste)	
		User ID	
		Key ID	0x
		Key Type (bit)	
		Key Size	
		Expiration	
		Fingerprint	
	[Note: Please include one public key block for all team members here.]		
		User ID	
		Key ID	0x
		Key Type (bit)	
		Key Size	
		Expiration	
		Fingerprint	
	[Note: Please include one public key block for all team members here.]		

Please provide information of your sponsor(s) ***Note: NOT applicable for fellows membership application***		
Sponsor 1		
Name of Sponsor	:	
Sponsor's Organization	:	
Phone/Fax	:	
Contact Email	:	
Sponsor 2		
Name of Sponsor	:	
Sponsor's Organization	:	
Phone/Fax	:	
Contact Email	:	

Organisation of Islamic Cooperation - 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 …………………………………………………………………………………… ……………………………………………………………………………………	

Filled and verified by Applicant’ Sponsor

……………………………………………………

Name:

Designation:

Date:

CODE OF ETHICS FOR MEMBERS

THE ORGANISATION OF ISLAMIC COOPERATION – COMPUTER EMERGENCY RESPONSE TEAM (OIC-CERT)

1.0 GENERAL

Members of the OIC-CERT shall maintain their memberships by adhering to the OIC-CERT Membership Code of Ethics. Members who intentionally or knowingly violate any terms of the Code will be subjected to action by a panel appointed by the Board, which may result in the revocation of the membership.

There are four fundamental elements in the code, and additional descriptions provided for each of the element are guidelines that may be considered by the OIC-CERT Committees in judging the behaviors of the members. It is intended to help members to identify and resolve the inevitable ethical dilemmas that they will confront during their tenure in the OIC-CERT. Therefore, strict adherence to this Code is important as a condition of the membership.

2.0 OBJECTIVES

The Code of Ethics for OIC-CERT members are set to achieve the following objectives:

a. Providing guidance for resolving good and bad behavior and practices.
b. Encouraging the right way of personal conducts by members.
c. Ensuring the right practices in all aspects of the OIC-CERT activities.
d. Encouraging members to adopt the right behavior that may create confidence and trust towards the OIC-CERT.
e. Discouraging behavior that may raise unnecessary doubt among members.
f. Preventing members from giving unwarranted comfort or reassurance.
g. Preventing members from exercising bad practices.
h. Preventing members from associating or appearing to associate with criminals or criminal behavior.

i. Preventing members from practicing bad behaviors that may give bad impressions towards the OIC-CERT.
j. Safeguarding the image of the OIC-CERT.

3.0 FUNDAMENTAL ELEMENTS

There are four fundamental elements under the Code of Ethics namely:

a. Protect the society, the organizations, and the infrastructure.
b. Act honorably, honestly, justly, responsibly, and legally.
c. Provide diligent and competent service.
d. Advance and protect the profession.

Compliance with the four fundamental elements is mandatory. Conflicts between the fundamentals should be resolved in the order of the fundamentals. The fundamentals are not equal and conflicts between them are not intended to create ethical binds.

3.1 Protect Society, Organization, and Infrastructure.

- Promote and preserve public trust and confidence in the information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.
- Restrict internal communication should not be disclosed.

3.2 Act Honorably, Honestly, Justly, Responsibly, and Legally

- Tell the truth; make all stakeholders aware of actions taken on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.

- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

3.3 Provide Diligent and Competent Service to others

- Preserve the value of the systems, applications, and information.
- Respect the trust and the privileges that are granted.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

3.4 Advance and Protect the Profession

- Sponsor for professional advancement to those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.