Cour
Pénale
Internationale

International
Criminal
Court

Le Bureau du Procureur
The Office of the Prosecutor

TERMS OF REFERENCE – Cyber Forensic Investigator / Cybersecurity

1. Operational Context

The Information, Knowledge and Evidence Management Section (IKEMS), headed by an Information Management Coordinator, reports directly to the Prosecutor, and combines the OTP's information, knowledge and evidence management operations into one consolidated section. IKEMS aims to maintain a coordinated, flexible and operationally responsive IKEM support capacity throughout the OTP, in order to support the full spectrum of OTP information and evidence operations.

The position of Cyber Forensic Investigator / Cybersecurity is part of the Cyber Unit (CU) of the Information, Knowledge and Evidence Management Section (IKEMS) which:

a) Provides user and information management support to OTP core businesses and systems such as investigations and witness management;

b) Conducts comprehensive business analyses, process mapping, requirements gathering, as well as business needs assessment exercises on behalf of the Prosecutor for all OTP business streams and leads a balanced and transparent approach toward OTP business development and innovation;

c) Supports OTP business development initiatives by ensuring continuous and recurring in-house program and project evaluation, as well as intra and inter-Organ sharing of lessons learnt in relation to IKEM;

d) Drafts and maintains the OTP's IKEM strategic plan, as well as forecast assessments of IKEM-related developments which may impact OTP core business or operations.

e) Supports existing knowledge- and information-management systems, business processes and eLearning needs within the Office by acting as the primary OTP knowledge broker in the IKEM area.

2. Tasks

Under the direct supervision of the Head of Cyber Unit and the overall management of the Information Management Coordinator, the incumbent will perform the following tasks:

<u>Digital Forensic Examination and Reporting:</u>

a) Conduct digital forensic examinations on computers, storage devices, and mobile devices.
b) Conduct data recovery operations to retrieve lost or deleted information while ensuring the integrity of the data.
c) Document and maintain a chain of custody for all collected digital evidence.
d) Analyse digital evidence, prepare detailed cyber forensic reports, and provide support for field activities.

Incident Response – Cyber Security Response:

a) Coordinate with the incident response team to contain, eradicate, and recover from security incidents.
b) Respond promptly to reported security incidents and conduct initial assessments.
c) Perform forensic analysis on digital devices, networks, and systems to identify and preserve evidence related to cyber incidents.
d) Stay updated on the latest cyber threats and vulnerabilities.
e) Integrate threat intelligence into investigative processes to enhance proactive detection and response capabilities.
f) Collaborate with IMSS, legal, and other relevant departments to gather information and facilitate investigations.
g) Provide expertise and support during legal proceedings

Specialize Online investigations support

Operational Support and Training:

a) Advise operational investigators on safe online investigation practices and the reliability of digital evidence.
b) Provide training/briefing to first responders and operational investigators on digital forensics.

Capability Development:

a) Contribute to the creation of operational forensic capabilities, including methodologies, equipment, and networks.

Advisory Role:

a) Advise and assist the Head of the Cyber Unit on all cyber and digital forensics-related matters, procedures, and techniques.

b) Perform tasks as instructed by the Head of the Cyber Unit, Coordinator of the Information, Knowledge and Evidence Management Section, and Director of Integrated Service Division.

<u>They will need to provide:</u>

a) Contribution to digital forensics resources.
b) Cyber examination capability.
c) Cyber Incident response
d) Specialized Online investigative activities
e) Quality control of delivered products.

3. Skills Required/Desired:

a) Professionalism, team spirit, diplomacy, flexibility, responsiveness, collaboration, and pedagogy.
b) Accuracy, reliability, diplomacy, politeness, understanding of the situation, and ethics.
c) Innovation, diplomacy, understanding of external parties' activities, professionalism, communication, and networking.
d) Diplomacy, sense of agreement, patience, flexibility, and firmness in non-negotiable forensic standards.
e) Strong understanding of cybersecurity principles, digital forensics, and incident response.
f) Proficiency in using forensic tools and techniques to analyze digital evidence.
g) Excellent communication skills, both written and verbal.
h) Ability to work independently and collaboratively in a team environment.
i) Strong problem-solving and critical-thinking skills.
j) Strong programming skills oriented to Digital forensics, Online Investigations or Cybersecurity.