Terms of Reference – Information Technology Security Officer (ITSO)

1. POST TITLE: HMS SULTAN ITSO

2. PREAMBLE AND AIM FOR THE HMS SULTAN ITSO:

The Information Security Officer (ITSO) is the first point of contact for all staff at HMS SULTAN regarding cyber and information security. The ITSO is responsible, through the Chain of Command for providing the Commanding Officer with assurance of effective cyber and information security management. The post is rank ranged OR9-OF2.

3. ON TAKING UP APPOINTMENT OF ITSO:

a. The new incumbents first action will be to conduct 100% muster of all assets within HMS SULTAN and to reconcile the assets against the Navy Command Asset Register (NCAR) or equivalent.

b. Register personal details with Air-CyISOC-SOC-Ops-GpMail@mod.gov.uk

c. Complete all mandatory training as defined in paragraph 8.

4. MAIN RESPONSIBILITIES OF ITSO:

a. To develop and implement local Cyber Security Policy and Procedures (CSPP) for their specific AOR where required. This will be in developed from MOD and Air CSPP.

b. Manage the Cyber Security of all non-MODNET assets within their AOR and scope.

c. Updating and maintaining the Cyber Threat Analysis Tool (CTRA) ensuring that all non-MODNET assets including but not limited to Portable Electronic Devices (PEDs), Tablets, Cameras, Printers are status recorded when they are received, returned or destroyed.

d. Understand the accreditation process and the Defence Assurance Risk Tool (DART) in order to guide submitters within HMS SULTAN through the process.

e. Act as focal point for triaging, actioning, and responding to MODCERT Directives.

f. Ensure that all the assets within their AOR are accredited and maintained throughout life. Retain a copy of all Accreditation Certificates and Security Operating Procedures (SyOPs).

g. Ensure anti-virus updates and patches are carried out within the required timeframe and in accordance with SyOPs. Contacting MCSU Service Desk with any issues.

h. Retain a copy of all master passwords for the assets within their AOR. These will be held in a cabinet / blister box controlled by the Unit Security Officer (USO).

i. The ITSO will support the USO when a monthly 10% spot check of all Cyber assets within their AOR is carried out. By the end of the year a 100% check will have been carried out.

j. Ensure all Information and Cyber breaches are reported to Air / Navy WARP through a Security Incident Reporting Form regardless of whether they were resolved at local level.

k. When required, monitor and / or assist with investigations into significant Cyber incidents.

l. Ensure that HMS SULTAN has a Cyber Champion to act as an ambassador through upholding of good security hygiene and maintaining a positive security culture by providing security advice and guidance, delivering education and awareness briefs.

m. Carry out annual Cyber assurance of holdings, policy, and procedures of subordinate units where applicable.

n. Provide support to all visits where Cyber assets are involved. These may be from, but not limited to Air CyISOC, Air PSyA, SCIDA.

o. Ensure that all Cyber related changes to PSyA (Air) Directives, Security Advisory Briefs, Air CyISOC directives are distributed to all department heads within HMS SULTAN.

p. Where necessary, to produce up to date instructions for assets, e.g. Printers, scanners, fax machines etc.

q. To conduct HMS SULTAN OOD duties as detailed.

r. To be available for whole ship duties as detailed and required by HMS SULTAN Executive Officer

5. KEEP UP TO DATE:

On Cyber Security via:

a. National Cyber Security Centre

b. Air Cyber and Information Services Operations Centre (AirCyISOC) web page

6. RESPONSIBLE TO:

Commanding Officer HMS SULTAN via Unit Security Officer.

7. AUTHORITY:

a. The ITSO is responsible to ensure that the HMS SULTAN chain of command is fully aware of any Cyber issues that may affect their output or compromise their information asset(s).

8. TRAINING - Qualifications required for the post:

a. **Essential** competence (which can be obtained once in post if not already in possession of):

i. Defence IT Security Officer (DITSO) (delivered at Chicksands – 3-4 days)

ii. Cyber 101 (DLE)

b. Desirable:

i. Cyber Foundation Pathway Module Zero (Part A conducted on DLE. Part B takes place at Defence Academy Shrivenham)

ii. Information Assurance Risk Management for HMG (delivered at Defence Academy - 2 days).