(d) Device ID.

The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this then the equipment must be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures are to be implemented:

(1). Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations),

(2). Defined Business Contingency Plan,

(3). Data backup with local storage,

(4). Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),

(5). Operating systems, applications and firmware should be supported,

(6). Patching of Operating Systems and Applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners. Wherever possible, a "Logon Banner" will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:

"Unauthorised access to this computer system may constitute a criminal offence"

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems must not be connected direct to the Internet or "un-trusted" systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).

k. Disposal. Before IT storage media (e.g. disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Laptops

60.25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 60.17 above.

60.26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites[1]. For the avoidance of doubt the term "drives" includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

60.27. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

60.28. Portable CIS devices holding the Authorities' data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

60.29. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE material to the Authority. In addition any loss or otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

JSyCC WARP Contact Details

Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)

RLI Email: defencewarp@modnet.rli.uk (MULTIUSER)

Telephone (Office hours): +44 (0) 30 6770 2185

JSyCC Out of hours Duty Officer: +44 (0) 7768 558863

Mail: JSyCC Defence Industry WARP

X007 Bazalgette Pavilion,

RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

60.30. Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf

Sub-Contracts

60.31. Where the Contractor wishes to sub-contract any elements of a Contract to sub-Contractors within its own country or to Contractors located in the UK such sub-

contracts will be notified to the Contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

60.32. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (third party) country. The first page of Appendix 5 (MOD Form 1686 (F1686) of the GovS 007 Security Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

60.33. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 60.31 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Publicity Material

60.34. Contractors wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.

Physical Destruction

60.35. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

60.36. Advice regarding the interpretation of the above requirements should be sought from the Authority.

60.37. Further requirements, advice and guidance for the protection of UK classified information at the level of UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

https://www.gov.uk/government/publications/industry-security-notices-isns

Audits

60.38. Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Contractors' National/Designated Security Authorities or the Authority to ensure compliance with these requirements.

61. Incentives/Gainshare

Incentives

61.1. The Contractor shall be incentivised to achieve and maintain the required level of performance through provisions of Clause above and through the monitoring of the Key Performance Indicators at Clause 23 above.

Gainshare

61.2. Both parties acknowledge that there is an agreed baseline for the Firm price agreed under this Contract, as set out in Schedule 1 (Schedule of Requirements), and that changes to that baseline which lead to cost reductions shall represent a Gainshare proposal.

61.3. The Gainshare Framework Agreement at Schedule 20 to this Contract details the possible, but not exclusive, areas for which the Authority and the Contractor shall work together to realise potential opportunities for increased efficiency and savings under the Contract.

61.4. All savings achieved, as a result of the Gainshare Framework Agreement at Schedule 20 to this Contract, shall be shared on an agreed basis between both parties, subject to the following:

61.4.1. any non-recurring costs incurred during investigation and subsequent implantation of any agreed Gainshare arrangement shall be offset against the agreed saving prior to the sharing of savings apportionment; and

61.4.2. any non-recurring costs incurred during investigating a proposed Gainshare, which has been approved by the Authority but at a later date it is agreed not to pursue for a reason listed in the Framework Agreement, shall be allowed a s a genuine charge to the Contract. No profit shall be permitted to be claimed when recovering non-recurring costs under the Gainshare proposal.

61.5. Any successful Gainshare Opportunities shall be implemented by formal amendment to the Contract following agreement by the Authority and the Contractor.

61.6. The Contractor shall, where appropriate, flow down the principles of Gainshare in his Contracts with Sub-Contractors and suppliers used in the performance of this Contract.

62. Social Value

62.1. No later than three (3) months from the Commencement Date, the Authority and Contractor will agree a set of Key Performance Indicators to monitor the commitment your organisation is making under each Social Value theme at Schedule 16A (Social Value – Tackling Economic Inequality), Schedule 16B (Social Value - Fighting Climate Change) and Schedule 16C (Social Value - Equal Opportunity) to ensure that opportunities under the contract are being delivered.

63. Limitations on Liability

Definitions

63.1. In this Clause 63 the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

"Charges" means any of the charges for the provision of the Services, Contractor Deliverables and the performance of any of the Contractor's other obligations under this Contract, as determined in accordance with this Contract;