A Security Aide-Memoire

BAE SYSTEMS

Contents

Introduction

BAE Systems' sites are in the main approved by government to work on classified contracts. The requirements placed upon us are more stringent than for most business environments. This aide-memoire only provides general information, for more detailed information please refer to the Security Service website:

http://www.maa.intranet.bae.co.uk/content/securityservices/default_3.htm

General points

- Do apply the clear desk policy, i.e. don't leave protectively marked or Company sensitive information out on your desk.
- Do wear and display your personal identity tag with the face clearly visible at all times whilst on site.In the event of loss please report this immediately to your Security department.
- Don't allow people you don't know to tailgate through access controlled doors.
- Don't write down passwords or combinations.
- Don't share your IT account with anyone else and either log off or lock your PC when unattended.
- Don't leave your laptop computer on either your desk overnight or visible in your car at any time.

Official information

The UK Government defines official information as any information (written or oral), document (printed or in electronic format) or article (such as an item of equipment) that comes into your possession during the course of your work as a defence contractor. It does not have to be protectively marked.

PROTECTIVELY MARKED = CLASSIFIED

Official Secrets Acts (OSA)

The Official Secrets Acts 1911-1989 applies to us all. As a defence contractor we are regularly working with official and protectively marked material and therefore everyone should be aware of the Acts. The Acts cover not just espionage but the failure to safeguard official information. If you don't know about the OSA read the guidance on the Security Services website.

DEFCON 659

A defence contract condition applied by the MOD to contracts CONFIDENTIAL and above. The condition details security measures that requires:

- Authority for disclosure of information.
- Material to be safeguarded to defined standards.
- Records of access to material to be obtained.
- Any failure to comply to be reported.
- Information to satisfy compliance to be provided.
- Right of inspection by at any time.

It also provides for termination of contract if the contractor is found in breach.

Government protective markings used in the UK

Staff involved with protectively marked material need to ensure that they fully understand how this information is processed and protected, advice can be found on the Security Service website and through your on site Security department. The mishandling of such material can have a serious and damaging effect on the business and may result in a breach of the Official Secrets Acts.

There are four protective markings used by the UK Government. Their defence definitions as follows:

- TOP SECRET would be likely to cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations.
- SECRET would be likely to cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations.
- CONFIDENTIAL would be likely to cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations.
- RESTRICTED would be likely to make it more difficult to maintain the operational effectiveness or security of UK or allied forces.

Company protective markings

Only two protective markings are used to safeguard sensitive BAE Systems' information:

- COMMERCIAL-IN-SECRET - When unauthorised disclosure would likely cause serious damage to the interests of the Company.
- IN STRICT CONFIDENCE - Unauthorised disclosure would likely be prejudicial to the interests of the Company.

Storage requirements

Information marked CONFIDENTIAL or above or COMMERCIAL-IN-SECRET must be kept in approved secure containers, registered and be accounted for at all times.

RESTRICTED or IN STRICT CONFIDENCE information must be kept under lock and key.

Full details of the protective measures can be found on the Security Services website.

Release of protectively marked or official information

If you need to release (i.e. send) official or protectively marked information outside the Company you are likely to require MOD approval prior to doing so. Seek advice from your Site Security Manager.

IT security

There are policies in place that govern how we use IT in BAE Systems.

You should familiarise yourself with the Company's Acceptable Use Policy and the relevant Security Operating Procedures.

- E-mail can be used to send information up to and including RESTRICTED or IN STRICT CONFIDENCE within Great Britain and only on the internal BAE Systems network.
- Commercially sensitive information may be sent by e-mail however transmissions must be encrypted – seek advice from your Site Security Manager.
- All laptops used to store or process either Company sensitive material or information up to RESTRICTED must be protected by suitable encryption – contact the Site Security Manager for detailed advice.

Security vetting

The Company Vetting Guide details the measures to be applied in obtaining assurances and clearance for individuals required to have access to sites and/or Company IT systems that hold protectively marked Information. The level of clearance will be determined by the level of access required.

The clearance levels most commonly found in the business are as follows.

- B.C. Basic Check.
- S.C. Security Check.
- D.V. Developed Vetting.

Visits to other companies or MOD sites in the UK

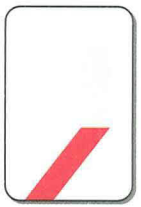
If you are visiting other companies or MOD sites to discuss protectively marked information it is likely that details of your security clearance need to be provided in advance of the visit. Your site security team have the capability to do this for you.

Personal identity tag

There are four types of pass used within BAE Systems as follows:

Employee cleared to SECRET

Contractor cleared to SECRET



Employee cleared to RESTRICTED or with limitations

Contractor cleared to RESTRICTED or with limitations

Homeworking

Homeworking on material no higher than RESTRICTED is permitted with the approval of your Line Manager. Detailed guidance can be found on the Security Services website.

Travelling overseas

Consider the following:

- Have you read the Security Services website for personal security advice while abroad and for the latest travel advice for the country that you are visiting?
- If you are visiting secure facilities or establishments abroad or are planning to discuss protectively marked information do you need to provide advanced notice of your security clearance? (Allow 6-8 weeks notice).
- Are you planning to carry any material that is either protectively marked or that may have a military or dual use application with you (including information held on your laptop)? You may need to obtain approval to do so (allow 5 working days notice).
- Do you have the 24-hour security travel advice telephone emergency number? **For travel emergencies call +44 207 942 9870** or check the website for further details.

For more information contact:

Basildon

Security Manager	Telephone 01268 883132
Security Control (24hrs)	Telephone 01268 883058

Edinburgh

Security Manager	Telephone 0131 3434115
Security Control (24hrs)	Telephone 0131 3434111

Plymouth

Security Manager	Telephone 01752 722013
Security Control (24hrs)	Telephone 01752 695695

Rochester

Security Manager	Telephone 01634 203444
Security Control (24hrs)	Telephone 01634 203281

Southampton

Security Manager	Telephone 02380 316751
Security Control (24hrs)	Telephone 02380 702300

Capability Green

Security Manager	Telephone 01582 886843
Security Control (24hrs)	Telephone 01582 795850

Travel Emergencies

Security travel advice (24hrs)	Telephone+44 207 942 9870

Security Service website:

http://www.maa.intranet.bae.co.uk/content/securityservices/default_3.htm

01.04.AV.001