Advice on the Management of External Visitors to Sensitive Sites

When external visitors (e.g. non-cleared individuals including foreign liaison, commercial competitors and the media) are due to visit a sensitive work location, we recommend the creation of a security plan in order to mitigate the security risks. This guidance is intended to help staff responsible for producing such a visit plan.

Before the visit

Ascertain necessity. Before agreeing to any visits to sensitive locations, consider whether they are really necessary. Will other options meet your business needs, such as conducting the visit in a non-sensitive location or using VTC or telephone conferencing technology?

Understand the threat. Those proposing, managing or participating in visits should be briefed on any relevant security threats. Threat information can come from a wide range of sources depending upon the nature of the visit - for example, from your internal security department, your local Counter Terrorism Security Advisor (CTSA) or your CPNI advisor.

Decide the access required. Once the threat is better understood, planners should consider what sites/areas of the business are suitable for the visitors to access. Where are they not to be allowed access? How will this be managed? Escorting visitors at all times is likely to be a key measure. We also recommend the use of passes to identify visitors and their level of site access. If available, use access control systems but do not rely upon these alone - escorting is always likely to be necessary.

Identify sensitive assets. Consider which assets within the areas to be accessed are sensitive and require protection. For example, visitors may be allowed into a room containing sensitive IT systems, wall charts or documents etc. The plan should highlight the steps to be taken to protect those sensitive assets, whether through their removal or by hiding them from view.

Inform visitors. The plan should state what visitors are required to bring with them (such as approved identification) and what they may not bring or will have to surrender on entry (such as
mobile telephones, IT, recording devices, cameras etc.). There may also be a requirement to confirm the visitors’ security clearance (for example, the level of National Security Vetting they hold). Communicate this clearly to the visitors prior to their arrival and enforce it on the day of the visit. We recommend that visitors are prevented from bringing bags into the sensitive environment.

**Define responsibilities.** Appoint a central point of contact for the management/reporting of any incidents during the visit. This should be a person without any responsibility for escorting the visitors, so that everyone can concentrate on their specific roles.

**Document and communicate.** The visit plan should be documented and communicated effectively to all personnel involved. In addition, all other members of staff within the locale of the visit should be told that a sensitive visit is taking place and what is expected of them. This enables them to act as further eyes and ears in respect of any suspicious activity and empowers them to report it if they see it.

**After the visit**

**Confirm the return of assets.** At the end of the visit all visitor passes and organisation assets should be returned under a managed process. Confirm that this has been done and all visitors have left.

**Consider an inspection.** Consider implementing an inspection of the areas visited, by staff familiar with those areas. This would include, for example, a physical check for the presence of things such as key-loggers or other unauthorized IT, for the unauthorized removal of any assets or any damage. The checks should be recorded in a register (possibly a page attached to the visit plan) for the corporate record. This should tie in with the visitor logs.

**Debrief staff.** Consider debriefing all involved staff to discuss any issues arising from the visit. This is principally to highlight any security concerns but can also be used to improve the management of future visits from an administrative perspective. Any security concerns should be appropriately acted upon and resolved when raised. During this process it may also be useful to discover whether any specific areas appeared to be of interest to the visitors, in case that highlights any concerns. Finding out what contact the visitors had with members of staff may be of interest from a social engineering perspective. This might include, for example, visitors providing a business card or attempting to instigate a friendship. During this process, consideration will need to be given to the appropriate security advice and guidance, which in turn will be informed largely by the threat (as discussed prior to the visit).

Further advice on the implementation of this guidance can be sought from your CPNI advisor.