<Company Name>
Visitor and Contractor Premise Access Policy

Created for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu.

1.0 Purpose
The purpose of this document is to provide guidance for Visitors to <Company Name> premises, as well as for employees sponsoring Visitors to <Company Name>.

2.0 Cancellation or Expiration
The processes and statements in this document do not have an expiry date. However, this document is reviewed and updated annually, and is maintained in the Document Management system of <Company Name>.

3.0 Background
<Company Name> is an Engineering and Manufacturing company, delivering quality engineered video products to our customers. As such, we have a significant investment in Intellectual Property. Also, our manufacturing facilities have areas that could be considered hazardous to untrained or unequipped personnel. This document provides the mechanism to protect both our Visitors and the company, while still filling our mandate of community education and participation.

4.0 Scope
This policy applies to all Visitors to any premise of <Company Name>, and to employees who sponsor Visitors.

5.0 Policy Statement
5.1 Parking
Visitors are encouraged to use designated Visitor Parking spots. If these spots are in use, regular employee parking spots can be used.

5.2 Check-In
All Visitors must arrive at a designated Check-In entrance (the main reception desk in most locations).

All Visitors must present government-issue photo identification at time of Check-In.

All Visitors must be met by their employee sponsor at the time of Check-In.

A Visitor cannot sponsor another Visitor.

Pets are not permitted; however, assistance animals such as Seeing Eye Dogs are permitted. In some cases prior arrangements may be required. Some manufacturing areas (such as assembly clean rooms) are not appropriate for animals under any circumstances.

Visitors must sign two copies of a "Visitor Agreement." Visitors must read this document and keep their copy of this agreement with them at all times during their visit. Visitors will be required to initial the ***Emergency Evacuation*** section of this agreement, and will be asked verbally if they have read and understand this section. Visitors will also be required to initial the ***Exit Inspection*** section of this document.

All Visitor electronics (laptops, other computer equipment, cell phones, etc.) will be checked in as described in the *Laptop, Computer and Related Equipment Check-In / Check-Out Procedure*.

5.3 Visitor Badges
Visitor Badges must be worn at all time. Employees are instructed to immediately report anyone not wearing a Visitor or Employee badge.

Visitors requiring access to areas controlled by swipe card access locks should arrange temporary cards with their sponsor. Departments that have swipe card access locks in their area may have a small number of temporary swipe cards available. These cards are limited to activation windows of 24 hours.

5.4 Photographs and Cameras
Visitors are not permitted to take photographs inside of <Company Name> premises, unless discussed specifically with sponsoring employees. For instance, photographs are sometimes required for documentation purposes. If employees have any questions about the suitability of photographs, they should consult the Human Resources Department.

Dedicated cameras are not permitted onsite. Cell phones and laptops equipped with cameras are permitted, but as previously stated photographs are not permitted without permission.

5.5 Information Disclosure
Visitors should not request information that does not pertain to their visit or the work being performed. confidential or otherwise inappropriate nature, requests for corporate documents, customer information, financial projections, comments on any matter currently under litigation, future products or future corporate direction, or requests for information or statements in the name of the company (as might be requested by a reporter or a lawyer) will be reported to the Office of the CSO, and will be dealt with under the "Penalties" section of this document.

5.5 Check-Out
Visitors will check out at the same station where they arrived. All Visitor electronics will be checked out individually as described in the Laptop, Computer and related equipment Check-In / Check-out Procedure. The checked out Visitor will be taken off the On-Premise List, both in the paper and online copies.

Checking out of computers and related equipment may take significantly longer after regular business hours, Visitors should factor this into their estimates for exit times.

5.6 Exit Inspection
Visitors may be subject to a brief search of their laptop bags or other luggage as they exit the premise. Permission for this search is granted by the Visitor signature on the Visitor Agreement Form (see the Check-In section of this document).

5.8 Emergency Evacuation
In the event of an emergency, it is the sponsoring employee's responsibility to ensure that the Visitor remains in the Evacuation marshalling area.

Emergency Coordinators will tally all Visitors using the Visitor Check-In information (using either the preferred online method or the fall-back paper sheets). *Visitors will not leave the property until it is confirmed with the Emergency Coordinators that they have successfully evacuated the building.*

5.9 Multiple Day Visits and Longer Term Contracts
Visitors who are at <Company Name> for multiple days must follow all procedures associated with this policy (Check-In, Check-Out, etc.) on each day of their visit. Longer term contractors can be sponsored for a photo-ID badge and would then fall under the Long Term Contractor Policy.

5.10 Visitors and Groups Requesting Tours of the Facility

All requests by groups for tours of <Company Name> facility will be referred to the Human Resources Department and/or the Office of the CSO for handling as an exception. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative.

In these cases, a verbal summary of the Emergency Evacuation Procedure and the restrictions on Photographs will be communicated to the Visitor Group prior to entry of the facility by a pre-designated <Company Name> employee. Any hazard specific to the areas being visited will also be communicated at that time. Visits to areas of this type may require waivers to be signed individually before entry to the facility.

All Visitors or Groups on a tour will be accompanied by their sponsor(s) at all times.

5.11 Network or System Access

Consultants or other Visitors that require internet network access can freely access the Visitor Wireless Network. Access to this network requires on-line agreement to the terms and conditions of network use. The unique number on the back of the Visitor badge is required to authenticate on the web page that is presented on access to this network.

Visitors who require access to production IT networks will need permission from their employee sponsor, who will arrange temporary credentials with the Helpdesk. Part of this procedure will require the Visitor to review the *Acceptable Use Policy*. After credentials are arranged, activities on the network will be subject to the Acceptable Use Policy. Visitor use of employee credentials is not permitted under any circumstances.

Visitors who require access to the production PLC or SCADA network will require prior permission from the Plant Manager and the Office of the CSO. Visitor use of employee credentials is not permitted under any circumstances.

Contractors making changes to production systems on either the IT or PLC/SCADA networks are subject to the IT and Production Systems Change Control Policy. In these cases, employee sponsors are required to review this policy with affected Visitors and ensure that the lead time and exceptions sections especially are clearly identified.

Remote Access to <Company Name> networks are governed by the <Company Name> Remote Access Policy.

5.12 On Courtesy

All employees of <Company Name> are to bear in mind at all times that all Visitors are either Customers or potential Customers. Even in the case of clear violations of this policy, all actions, dealings and conversations are to be courteous in nature.

6.0 Responsibility

This document is maintained jointly by the Human Resources Department and the Office of the CSO (Chief Security Officer).

Enforcement of this policy falls to these offices, as indicated in this document

Administration of the Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. In most facilities it is a duty of the main Reception Desk.

7.0 Penalties

Violation of any of the requirements in this policy by any employee will result in suitable disciplinary action, up to and including prosecution and / or termination.

Violation of any of the requirements in this policy by any Visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

8.0 Related Documents

The following documents are referenced in this policy.   It is the responsibility of employees sponsoring Visitors to <Company Name> to ensure that Visitors are compliant with all policies and procedures that apply to any activities and situations that occur while on-site. In some cases Visitors to <Company Name> may be asked to review, agree to, and in some cases sign one or more of these documents as part of their Check-In process.

- Visitor Check-In Procedure
- Visitor Check-In Agreement
- Laptop, Computer and related equipment Check-In / Check-out Procedure
- Emergency Evacuation Policy
- Emergency Evacuation Procedures (Note that this encompasses several documents)
- Visitor Network Access Agreement (online webpage, a paper copy of this agreement under revision control is maintained by and available from the Office of the CSO)
- IT and Production Systems Change Control Policy
- Network User Registration Policy
- Network User Registration Procedure
- Computer and Network Acceptable Use Policy
- Remote Access Policy

All Corporate Policies and Procedures are to be considered confidential information. While many of these Corporate Documents are required by Visitors as part of their visit, any policies or procedures not required in this capacity should be considered to be governed by the "Information Disclosure" section of this document.

9.0 Revision History

Version 1.0 – Rob VandenBrink	Date: 24 March 2010 Initial Version