

The Secured User Research Facility (S.U.R.F.), located on the Corporate campus in Mountain View, provides physical and electronic facilities for collaborative work between Synopsys and their business partners and/or customers in an environment designed to provide the protection of each company's intellectual property.

Synopsys uses this specially designed and maintained space as well as security and network technology to protect both Synopsys' and other parties' confidential information from unauthorized access or use. To insure the success of this facility, it is therefore important that the guidelines outlined below be followed.

- Users assigned to SURF (SURFers) are issued Orange Access Badges, which identify you as being SURFers and which provide for twenty-four hour access, seven days a week to the area. Access to the area after normal business hours is through the outside door only. Lobby access is unavailable by SURFers after business hours. SURFers must be escorted by a Synopsys employees after hours.
- Authorized Synopsys employees have access to the area during normal business hours Monday through Friday. At all other times, they are to be admitted by a hosting SURFer.
- Notify Security immediately if:
 - your badge or key code is stolen or stops working;
 - you discover that someone has had unauthorized access to your office, account or computer;
 - you discover any gaps or irregularities in physical security.
- The private break room and lavatory are private areas for SURF. Contractors supplying or maintaining these areas will be escorted or otherwise authorized.
- Use shredders and Confidential Bins, avoiding regular trash as appropriate.
- SURFers are responsible for reserving the conference room and removing any confidential information after such use, including erasing white boards.
- SURFers are responsible for security and access to their individual Synopsys office and computer account(s). Do not write key code, pin or computer passwords down anywhere on or near the Office or Access Badge.
- Report gaps or irregularities or problems in system or network security to NCS immediately. Network configurations have been designed to permit data flow between Synopsys' and customers' or partner's networks on a limited basis as authorized. Exploiting any such gaps in security is in direct breach of this Agreement.
- Authorize additional individuals access to your office by including them on the list at the end of this agreement.
- Respect the privacy of the other users of the facility.
- Respect the Federal, State and local laws which govern various aspects of computer and telecommunications use.

Violation of these rules may result in the revocation of user access to Synopsys, dismissal from Synopsys (when applicable) or other legal or civil penalties as appropriate. Access badges must be returned to Security upon termination of assignment to S.U.R.F.

By my signature below, I acknowledge that I have read and understand the guidelines listed above and agree to abide by these rules.

I _____ (PLEASE PRINT) AN EMPLOYEE OF
 _____, HAVE READ AND AGREE TO THE TERMS OF THIS
 ACCESS AGREEMENT EXECUTED BY MY HAND THIS _____ DAY OF _____,

200 ____ .

