Sensitive and Proprietary Information

The National Graduate School of Quality Management (NGS) takes seriously its obligation to protect sensitive and proprietary information and, therefore, utilizes a network of checks and balances that includes non-disclosure agreements, limited authorization and isolated electronic access. The NGS faculty, students and staff are bound by internal non-disclosure agreements (NDA's) as well as individual agreements with sponsors. NDA rules are also in effect during class discussions. Failure to follow any NDA agreement would result in the immediate expulsion of students and termination of faculty or staff members.

Proprietary Information

During the "process analysis" of a sponsoring organization, it may be necessary for that institution to provide proprietary information to ensure an accurate assessment of the current business process under review. Any information provided during the process improvement procedures remains the property of the sponsoring organization and may only be used according to the standards of confidentiality in place at the National Graduate School since 1993.

NGS students and faculty members may only use proprietary and sensitive information for the research-related activities under the strict and vigorously enforced institutional guidelines. No information shared by the sponsoring organization is made public without its written consent.

Classified Information

When a sponsor or Senior Champion(s) prefers that a project address sensitive or classified subjects, that individual must coordinate the effort directly with the institution through the Office of the President. The NGS leadership will ensure that the faculty member assigned to the Faculty Juried Review Team and all student team members possess the required level of clearance. NGS will follow the guidelines set forth by the sponsoring organization to ensure that classified information is shared only on a need-to-know basis. It is the convention of NGS to:

- Maintain all sensitive information on the organization's premises;
- Secure sensitive information in properly locked containers;
- Destroy sensitive information by utilizing a crosscut, high-security document shredder;
- Not transmit sensitive information over non-secure systems;
- Not leave sensitive information in voicemail accounts;
- Not discuss sensitive information in non-secure facilities;
- Not include sensitive information in public presentations