Information Security Policy

As part of information security policy, the Office of IT Services monitors the network usage by the students. The students of the University are strictly prohibited from engaging in any of the following acts:

- Causing a security breach to either CHRIST (Deemed to be University) network or any other network resources, including, but not limited to, accessing data, servers, or accounts to which they do not have authorized access; circumventing user authentication on any device; or sniffing network traffic, etc.
- Causing a disruption of service to either CHRIST (Deemed to be University) or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes, etc.
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
- Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, email bombs, spyware, adware, and keyloggers.
- Port scanning or security scanning on a production network unless authorized in advance by Information Security.
- Sending Spam via email, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

If the students are found engaging in any of the prohibited activities listed above, the University may initiate disciplinary actions including restricting access to campus network.