Legal

Table Of Contents

Confidentiality/Non-Disclosure Agreements

For more information about Confidentiality/Non-Disclosure Agreements, please see the Office of Legal Affairs website:

- Confidentiality/Non-Disclosure Agreements

Consulting

Consulting Agreements

For general information about Consulting Agreements and links to resources, please see the Office of Legal Affairs website:

- Consulting Agreements

Contracts

For information about:

- Contracting Issues - Legal Aspects
- Purchasing Contracts
- Research Contracts
- Presidential Signature Authority

EU General Data Protection Regulation Compliance Policy

Type of Policy: Administrative
Last Revised: Apr 2018
Review Date: Apr 2020
Policy Owner: Institutional Research & Enterprise Data Management
Contact Name: Katherine Crawford
Contact Title: Senior Director, Enterprise Data Management
Contact Email: katie.crawford@edm.gatech.edu
Reason for Policy:
The European Union has passed a data privacy regulation that is applicable throughout the entire European Union ("EU"), and to those who collect personal data about people in the EU. The European Union General Data Protection Regulation ("EU GDPR") imposes obligations on entities, like Georgia Tech, that collect or process personal data about people in the EU. The EU GDPR applies to personal data collected or processed about *anyone located in the EU*, regardless of whether they are a citizen or permanent resident of an EU country.

Georgia Institute of Technology ("Georgia Tech" or the "Institute") is an institute of higher education involved in education, research and community development. In order for Georgia Tech to educate its foreign and domestic students both in class and on-line, engage in worldclass research, and provide community services, it is essential and necessary, and Georgia Tech has a lawful basis, to collect, process, use, and/or maintain the personal data of its students, employees, applicants, research subjects, and others involved in its educational, research, and community programs. These activities include, without limitation, admission, registration, delivery of classroom, on-line, and study abroad education, grades, communications, employment, applied research, development, program analysis for improvements, and records retention.

Georgia Tech takes seriously its duty to protect the personal data it collects or processes. In addition to Georgia Tech's overall data protection program, Georgia Tech must make sure it complies with the dictates of the EU GDPR. Among other things, the EU GDPR requires Georgia Tech to:

a. be transparent about the personal data it collects or processes and the uses it makes of any personal data
b. keep track of all uses and disclosures it makes of personal data
c. appropriately secure personal data

This policy describes Georgia Tech's data protection strategy to comply with the EU GDPR.

Policy Statement:
2.1 Lawful Basis for Collecting or Processing Personal Data

Georgia Tech has a lawful basis to collect and process personal data. Most of Georgia Tech's collection and processing of personal data will fall under the following categories:

a. Processing is necessary for the purposes of the legitimate interests pursued by Georgia Tech or by a third party.
b. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
c. Processing is necessary for compliance with a legal obligation to which Georgia Tech is subject.
d. The data subject has given consent to the processing of his or her special categories of sensitive personal data for one or more specific purposes.

There will be some instances where the collection and processing of personal data will be pursuant to other lawful bases

2.2 Data Protection & Governance

Georgia Tech will protect all personal data and special categories of sensitive personal data that it collects or processes for a lawful basis. Any personal data and special categories of sensitive personal data collected or processed by Georgia Tech shall be:

a. Processed lawfully, fairly, and in a transparent manner
b. Collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes
c. Limited to what is necessary in relation to the purposes for which they are collected and processed
d. Accurate and kept up to date
e. Retained only as long as necessary
f. Secure

2.3 Sensitive Personal Data & Consent

Georgia Tech must obtain consent before it collects or processes special categories of sensitive personal data.

2.4 Individual Rights

Individual data subjects covered by this policy will be afforded the following rights:

a. information about the controller collecting the data

b. the data protection officer contact information (if assigned)
c. the purposes and lawful basis of the data collection/processing
d. recipients of the personal data
e. if Georgia Tech intends to transfer personal data to another country or international organization
f. the period the personal data will be stored
g. the existence of the right to access, rectify incorrect data or erase personal data, restrict or object to processing, and the right to data portability
h. the existence of the right to withdraw consent at any time
i. the right to lodge a complaint with a supervisory authority (established in the EU)
j. why the personal data are required, and possible consequences of the failure to provide the data
k. the existence of automated decision-making, including profiling
l. if the collected data are going to be further processed for a purpose other than that for which it was collected

Note: Exercising of these rights is a guarantee to be afforded a process and not the guarantee of an outcome.

Scope:
This policy applies to the personal data and special categories of sensitive personal data protected by the EU GDPR and all Georgia Tech Units who collect or process personal data and special categories of sensitive personal data protected by the EU GDPR.

Definitions:

Collect or Process Data	Collection, storage, recording, organizing, structuring, adaptation or alteration, consultation, use, retrieval, disclosure by transmission/dissemination or otherwise making data available, alignment or combination, restriction, erasure or destruction of personal data, whether or not by automated means.
Consent	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Under the EU GDPR: a. Consent must be a demonstrable, clear affirmative action. b. Consent can be withdrawn by the data subject at any time and must be as easy to withdraw consent as it is to give consent. c. Consent cannot be silence, a pre-ticked box or inaction. d. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. e. Request for consent must be presented clearly and in plain language. f. Maintain a record regarding how and when consent was given.

Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Georgia Tech Unit	A Georgia Tech college, school, office or department.
Identified or Identifiable Person	An identified or identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that person. Examples of identifiers include but are not limited to: name, photo, email address, identification number such as GT ID#, GT Account (User ID), physical address or other location data, IP address or other online identifier
Lawful Basis	Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: a. The data subject has given consent to the processing of his or her personal data for one or more specific purposes; b. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c. Processing is necessary for compliance with a legal obligation to which the controller is subject; d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person; e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.
Legitimate Interest	Processing of personal data is lawful if such processing is necessary for the legitimate business purposes of the data controller/processor, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
Personal Data	Any information relating to an identified or identifiable person (the data subject).
Processor	A natural or legal person, public authority, agency or other

	body who processes personal data on behalf of the controller.
Special Categories of Sensitive Personal Data	Special categories of sensitive personal data that require consent by the data subject **before** collecting or processing are: a. Racial or ethnic origin b. Political opinions c. Religious or philosophical beliefs d. Trade union membership e. Genetic, biometric data for the purposes of uniquely identifying a natural person f. Health data g. Data concerning a person's sex life or sexual orientation

Procedures:

5.1 Data Governance	
Document Lawful Basis for Collection or Processing	All Georgia Tech Units who collect or process personal data protected by the EU GDPR must document the lawful basis for the collection or processing of personal data and special categories of sensitive personal data they collect or process, why they collect it, and how long they keep it using the online **Georgia Tech EU GDPR Lawful Basis Form:** http://eugdpr.gatech.edu/georgia-tech-compliance All data at Georgia Tech shall be kept in compliance with the USG-BOR Records Retention Schedules.
5.2. Privacy Notice	
Georgia Tech's Privacy Notice	Georgia Tech's Privacy Notice to data subjects must specify the lawful basis for Georgia Tech to collect or process personal data and include: a. whether their personal data are being collected or processed and for what purpose b. categories of personal data concerned c. to whom personal data is disclosed d. storage period (records retention period) e. existence of individual rights to rectify incorrect data, erase, restrict or object to processing f. how to lodge a complaint g. the source of the personal data (if not collected from the data subject) h. the existence of automated decision-making, including profiling A link to the Georgia Tech Privacy Notice is available on the footer of all Georgia Tech websites – "Legal & Privacy

5.2. Privacy Notice	
	Information": http://www.gatech.edu/privacy
Georgia Tech Units Privacy Notice	Each Georgia Tech Unit that collects or processes personal data protected by the EU GDPR must create and publicly post a privacy notice that meets the requirements (a) through (h) set forth above. A link to the Georgia Tech Unit Privacy template is available at: http://eugdpr.gatech.edu/georgia-tech-compliance
5.3 Consent	
Documentation of Consent	Georgia Tech Units must obtain affirmative consent before it collects or processes sensitive personal data. **Georgia Tech EU GDPR Model Consent Form**: http://eugdpr.gatech.edu/sites/default/files /documents/eu_gdpr_consent_form_for_sensitive_personal_data.docx
Withdrawal of Consent	Georgia Tech must have a process for individuals who request to withdraw their consent.
5.4 Individual Rights	
Exercise of Rights	Any individual wishing to exercise their rights under this policy should contact Institutional Research & Enterprise Data Management: eugdpr@edm.gatech.edu
5.5 Data Protection	
Security of Personal Data	All personal data and special categories of sensitive personal data collected or processed by any Georgia Tech Units under the scope of this policy must comply with the security controls and systems and process requirements and standards of NIST Special Publication 800-171 as set forth in the Georgia Tech Controlled Unclassified Information Policy found here: https://policylibrary.gatech.edu/information-technology/controlled-unclassified-information
Breach Notification	Any Georgia Tech Unit that suspects that a breach or disclosure of personal data has occurred must **immediately** notify Georgia Tech Cyber Security here: https://security.gatech.edu/report-incident

Form Links:
EU GDPR Lawful Basis Form
EU GDPR Model Consent Form
EU GDPR Georgia Tech Unit Privacy Notice
Frequently Asked Questions: For Frequently Asked Questions about EU GDPR compliance at Georgia Tech
Responsibilities:

8.1 Responsible Party:

Georgia Tech Units
To document the lawful basis for personal data or special categories of sensitive personal data collected or processed pursuant to this policy.

To cooperate with Institutional Research & Enterprise Data Management when individuals inquire about their personal data or special categories of sensitive personal data collected or processed pursuant to this policy (See Section 2.3).

To immediately notify (24/7) and cooperate with Georgia Tech Cyber Security relating to any data breach: https://security.gatech.edu/report-incident

8.2 Responsible Party:

Institutional Research & Enterprise Data Management
To field inquiries about personal data or special categories of sensitive personal data collected from individuals while in the EU (See Section 2.4).

To coordinate with Georgia Tech Unit responding to inquiries about personal data or special categories of sensitive personal data collected from individuals while in the EU.

8.3 Responsible Party:

Cyber Security
To answer questions about and review data security measures.

To handle data breach notification for the Institute.

Enforcement:
Violations of the policy may result in loss of system, network, and data access privileges, administrative sanctions (up to and including termination or expulsion) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

To report suspected instances of noncompliance with this policy, please contact Institutional Research & Enterprise Data Management at: eugdpr@edm.gatech.edu, or visit Georgia Tech's *EthicsPoint*, a secure and confidential reporting system, at: https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7508

Enforcement of the EU GDPR shall be carried out by the appropriate Data Protection Authority within the European Union.

Related Information:
EU General Data Protection Regulation (EU GDPR)
EU GDPR FAQs
Georgia Tech Legal & Privacy Notice
Georgia Tech Data Protection Safeguards
Georgia Tech Controlled Unclassified Information Policy
NIST Special Publication 800-171
USG-BOR Records Retention Schedules

Policy History:

Revision Date	Author	Description

05-03-2018	Institutional Research & Enterprise Data Management	New Policy

Export Issues and International Travel

For information about Export Issues and International Travel, please see:

- Export Issues - Legal Aspects
- Research Support Export Control

Intellectual Property and Copyright

Intellectual Property:

- Faculty Handbook 5.4 Intellectual Property Policy
- Intellectual Property Assignment Agreement
- Intellectual Property-Legal Aspects
- Patents-Legal Aspects

Copyright:

- Copyright & Fair Use at Geeorgia Tech
- Copyright Infringement Procedure
- Copyright-Legal Aspects
- USG Copyright Resources:
  - Copyright
  - Fair Use Exception
  - Fair Use Checklist

Minors on Campus

- Mandatory Reporting of Child Abuse Policy
- Youth Programs Policy
- Minors in Laboratories, Hazardous Areas and Animal Facilities Policy

For additional information regarding Minors on Campus, please see the Youth Programs website here.

Open Records Act Policy

Type of Policy: Administrative
Effective Date: Sep 2012
Last Revised: Sep 2012
Review Date: Sep 2019
Policy Owner: Office of Legal Affairs
Contact Name: Kate Wasch
Contact Title: Managing Attorney
Contact Email: asklegal@gatech.edu
Reason for Policy:

As a public institution, Georgia Tech is subject to the Open Records Act, O.C.G.A. § 50-18-70 et seq. The law requires that Georgia Tech make available for public inspection public documents within three business days of receiving a request. The purpose of this policy and its procedures is to ensure compliance with the law.

Policy Statement:
Georgia Tech must respond to Open Records Act requests as required by the Open Records Act, O.C.G.A. § 50-18-70 et seq. (the "ORA"). With limited exceptions, Georgia Tech must respond to such requests within three business days. In response to an ORA request, Georgia Tech will allow the requester to view public documents and, for a fee, make copies.

The Office of Legal Affairs ("OLA") has been designated by the President of Georgia Tech as the office responsible for responding to ORA requests on behalf of the custodian of the records. Departments and school, as custodians of Georgia Tech's records, must work in cooperation with OLA to ensure Georgia Tech's compliance with the ORA. The custodian of the records remains responsible for compliance with the ORA and for any civil or criminal penalties imposed for failure to comply.

Departments, schools, faculty or staff who receive an ORA request from any person, or an ORA inquiry from OLA, shall respond promptly, following the procedures in this policy.

Scope:
This Policy applies to all Georgia Tech departments, schools, faculty, and staff.

Policy Terms:
Public Records
All documents or other records (including video, audio, or electronic records) prepared or maintained by Georgia Tech, as well as documents prepared or maintained by its employees as part of their job responsibilities, are subject to the ORA. For example, employee notes of official University business (e.g., notes of meetings) are public, not personal, documents. The ORA includes "computer based or generated information" within the definition of a "public record." This includes, for example, e-mail and logs kept on a server.

Custodian
The person responsible for maintaining the records in the ordinary course of business.

Procedures:
See Office of Legal Affairs website: www.legal.gatech.edu.

Responsibilities:

The Office of Legal Affairs
OLA has been designated by the President of the Institute as the office responsible for responding to ORA requests.

Georgia Tech Departments and Schools
Georgia Tech departments and schools are responsible for maintaining their own records and for collecting and preparing requested documents in response to an ORA request.

Enforcement:
Any person who knowingly and willfully fails to respond to a written ORA request may be found guilty of a misdemeanor criminal act, and fined up to $1,000 for the first violation. Additional civil and criminal penalties may also be imposed.

Violation of this Georgia Tech policy may result in disciplinary action, up to and including termination of employment.

Related Information:
Georgia Open Records Act
BOR Policy Records Retention Schedule
Georgia Tech Office of Legal Affairs
FOIA
FERPA

Policy History:

Revision Date	Author	Description
04-17-2012	Office of Legal Affairs	Update per change in ORA law.
10-12-2012	Office of Legal Affairs	Established a formal written policy.

Presidential Signature Authority

Type of Policy: Administrative
Effective Date: Jul 2011
Last Revised: Nov 2015
Review Date: Nov 2018
Policy Owner: Legal Affairs and Risk Management
Contact Name: Patrick McKenna
Contact Title: Vice President, Legal Affairs and Risk Management
Contact Email: pat.mckenna@carnegie.gatech.edu
Reason for Policy:
The Board of Regents of the University System of Georgia (BOR) has delegated authority to the president of each system institution or their designee to execute certain types of agreements. This policy is intended to describe the process by which the President of the Institute may designate other Institute officials to execute, accept or deliver those agreements and the conditions under which the officials so designated are expected to act.

Policy Statement:
The President of the Institute may, by written delegation, designate additional officials of the Institute to assist in executing Agreements in the name of the Georgia Institute of Technology on behalf of the Board of Regents. A delegation of signature authority by the President shall apply to the incumbent in the position named in the delegation or in any position which replaces the named position.

The individual exercising the delegated signature authority is expected to execute, accept or deliver only those Agreements that are specified in the delegation and are within the purview of the individual's position. Each such individual should act with the concurrence and approval of the senior leadership of their respective unit.

Only those individuals designated by the President may execute, accept or deliver Agreements in the name of the Institute. A delegation of signature authority may not be further delegated.

Scope:
This policy applies to the execution, acceptance and delivery of Agreements, including those agreements necessary for the day-to-day operation of the Institute.

This policy does not apply to Purchasing Agreements which should be reviewed, approved and executed by Georgia Tech Purchasing.

Definitions:

Agreements	Those agreements described in the BOR policies (see Related Information below). The term includes any document entered into on behalf of the Institute in which the parties make legally enforceable commitments, whether or not titled a contract or agreement. Terms used to describe an Agreement may include letter of agreement, letter of intent, memorandum of understanding, consortium agreement, operating agreement, or equipment loan.
Purchasing Agreements	Agreements for the purchase of supplies, materials equipment and certain contractual services of $10,000 or more. Authority to commit Institute funds for these purposes has been delegated to Georgia Tech Purchasing within the limits established by the State Department of Administrative Services.

Procedures:

Delegation of Authority Memorandum	The President of the Institute may periodically issue a memorandum to confirm the conditions under which other officials of the Institute have been authorized to act in the place of the President. A Delegation of Authority Memorandum will supersede and replace all prior delegations.
Legal Affairs Review	A delegation of signature authority shall, unless otherwise specified, extend only to standard form agreements that have been developed by the Office of Legal Affairs or to specific agreements that have been reviewed by the Office of Legal Affairs.

Frequently Asked Questions: Office of Legal Affairs-FAQ's

Responsibilities:

Office of Legal Affairs. The Office of Legal Affairs (asklegal@gatech.edu) will assist in determining who is authorized to sign a specific Agreement.

Enforcement:

Violation of this policy may result in disciplinary action up to an including termination of employment. Under Georgia state law, individuals who sign without authority may incur personal liability for any contracts they sign.

Related Information:

Delegation of Authority Memorandum (GT Login Required)
Office of Legal Affairs - Signature Authority
BOR Policy 2.5 Presidential Authority and Responsibilities
BOR Policy 7.4 Private Donations
BOR Policy 7.9 Contracts
BOR Policy 7.11.8 Trademarks
BOR Policy 9.6 Facilities Contracting
BOR Policy 11.2 Information Technology Project Authorization
BOR Business Procedure 3.4 Contracts
Overview and Procurement Authority/Responsibility

Procurement Delegated Authority

Policy History:

Revision Date	Author	Description
07-18-2011	Legal Affairs & Risk Management	New Institute Policy
09-25-2012	Legal Affairs & Risk Management	Policy statement edited to limit scope to Presidential signature authority
11-23-2015	Legal Affairs & Risk Management	Updated policy

Security Camera Use

Type of Policy: Administrative
Effective Date: Apr 2018
Last Revised: Apr 2018
Review Date: Apr 2020
Policy Owner: Security and Police
Contact Name: Jeffrey Hunnicutt
Contact Title: Physical Security Specialist
Contact Email: jeff.hunnicutt@police.gatech.edu
Reason for Policy:
Video Management Systems (hereafter, “VMS”) and video surveillance devices are necessary to deter, detect and prosecute wrong-doing on the Georgia Tech Campus. This policy is necessary to ensure the effective, efficient, ethical, and legal use of the Institute’s VMS and video surveillance devices in: protecting sensitive or classified information; protecting Georgia Tech and personal resources; and identifying those responsible for committing criminal acts, safeguarding video evidence, and pursuing prosecution in accordance with the U.S. Constitution, United States Federal law, Georgia State law, City of Atlanta municipal ordinances, and Board of Regents and Institute policy.

Policy Statement:
The Institute’s employees, contractors, representatives, and others having responsibility for installing, maintaining, having access to, having the capability of viewing, or otherwise having the ability to utilize VMS and video surveillance devices associated with any real property owned, leased or occupied by the Institute, or any entity with a Georgia Tech affiliation, shall utilize said video surveillance devices in a manner consistent with the U.S. Constitution, United States Federal law, Georgia State law, City of Atlanta municipal ordinances, Georgia Tech Police Department’s (hereafter “GTPD”) “Video Surveillance” policy, and Institute “Ethics” policy.

Installation of any video surveillance devices shall be coordinated with either GTPD’s Physical Security Specialist or the Georgia Tech Research Institute’s (hereafter “GTRI) Research Security Department in order to ensure video surveillance devices are not placed or positioned in such a way as to compromise a person’s expectation of privacy. No one is authorized to install security controls, to include video surveillance devices, web cams or other intrusive electronic devices used for surveillance, without the proper coordination with either the GTPD or GTRI Research Security Department.

The installation and monitoring of all such video surveillance devices shall be solely for the legitimate purposes of protecting human life, personal property, and the Institute’s interests and assets.

Recorded images shall not be made public, nor shall recorded images be released to, provided to, or otherwise made accessible to, any person, party or entity inside or outside of the Institute, without the Institute’s express permission, or

as required by law.

All requests to obtain recorded images must be submitted through the Georgia Tech Police Department Records Division.

Scope:
This policy applies to all Institute Building Managers, Security Contractors, Security Equipment Installers, GTPD Employees, GTRI Employees, and all others with the capability of accessing, viewing or utilizing live or recorded images associated with the video surveillance devices on any Institute VMS.

Definitions:

Institute	The Georgia Institute of Technology
Video Surveillance Device	Any device capable of viewing, transmitting and/or capturing still or streaming video images, whether or not associated with monitoring or recording devices.
Video Management System	Also referred to as “VMS” - is any electronic system capable of receiving, displaying, capturing, and/or recording images transmitted by cameras, whether across a network or within a closed circuit.

Procedures:

5.1 Requests for Video	
Internal Requests for Video Footage	Submit an email request to the Georgia Tech Police Department’s Records Division. openrecords@police.gatech.edu
5.2 Installation of New Cameras	
New Construction & Building Renovations	http://gtlowvoltagestandards.gatech.edu/node/123
Adding Cameras to Existing VMS	Reference GTPD Video Surveillance System Policy 7-05c, 4.1
New VMS Installation Not Related to Construction or Building Renovation	Reference GTPD Video Surveillance System Policy 7-05c, 4.1

Form Links: GTPD Report Request Form
Frequently Asked Questions: See GTPD website at
Responsibilities:

Georgia Tech Police Department
The GTPD’s employees, as defined by the GTPD Video Surveillance System Policy, will be responsible for the day-to-day operational use, administration, and maintenance of the GTPD’s VMS, to include training, creation of accounts, assignment of user privileges, repair, and maintenance of video surveillance devices.

Georgia Tech Research Institute
GTRI's Research Security and Information Systems Department (ISD) will be responsible for the day-to-day administration and maintenance of their VMS, to include training, creation of accounts, assignment of user privileges, repair and maintenance of video surveillance devices, etc.

Enforcement:
Access to Georgia Tech's VMS and information via Georgia Tech computer systems is limited to those employees and faculty who have a legitimate business reason to access such information. The Institute has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security to Georgia Tech information systems.

Violations of the policies may result in loss of usage privileges, administrative sanctions (including disciplinary action) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

To report suspected instances of noncompliance with this policy, please contact GTPD or visit Georgia Tech's *EthicsPoint*, a secure and confidential reporting system, at: https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7508

Related Information:
University System of Georgia Ethics Policy
Acceptable Use Policy
Cyber Security Policy
Data Privacy Policy

Policy History:

Revision Date	Author	Description
April 2018	GTPD, Physical Security	New Policy

Software Licenses

For information about Software Licensing, please see:

- Software Licensing and Administration
- Software Licenses - Legal Aspects