Confidentiality.

All policies and password information remain the Confidential Information of Campus Management Corp. or Talisma Corporation Pvt. Ltd, as applicable. The sharing of passwords and policies with unauthorized third parties is strictly prohibited.

CAMPUSNET[SM] SERVICE, CMC SAAS, AND TALISMA SAAS ACCEPTABLE USE POLICY

This Acceptable Use Policy incorporates by reference all of the terms and conditions set forth in the Agreement.

CampusNet Service/CMC SaaS/Talisma SaaS information and resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to the CampusNet Service/CMC SaaS/Talisma SaaS operations, image, or financial interests and to comply with CMC's/Talisma's acceptable use policies and procedures as amended by CMC/Talisma from time-to-time.

CampusNet Service/CMC SaaS/Talisma SaaS users are required to notify CMC's/Talisma's CampusNet/SaaS Executive and Privacy Officer before engaging in any activities unrelated to the proper use of CMC/Talisma Software and not clearly addressed in this Acceptable Use Policy.

Designated Parties. The responsibilities of specific the CampusNet Service/CMC SaaS/Talisma SaaS personnel is shown in the following table, where "X" means a primary responsibility and "S" means a shared responsibility:

Activity	Privacy Officer	CampusNet/SaaS Executive	Customer Liaison	System Administrators	All Personnel
Develops Acceptable Use Policy	S	S			
Informs Customer of Policy	X	X	X		
Informs CMC/Talisma Staff of Policy	X	X		X	
Compliance with Use, Copyright and Licensing	X	X	X	X	X
Comply with Personally-owned Software Policy	X	X	X	X	X
Compliance Audits	S	S			
Protect Intellectual Property	X	X	X	X	X
Comply with Electronic Mail Policy	X	X	X	X	X
Comply with Electronic Mail Encryption Policy	X	X	X	X	X
System Monitoring				X	
Reporting Non-compliance	X	X	X	X	X

Privacy Officer.
The Privacy Officer is responsible for developing the CampusNet Service/CMC SaaS/Talisma SaaS policy with regard to privacy issues.

CampusNet Executive.
The CampusNet/SaaS executive, a CMC/Talisma employee, is responsible for:

a. Informing all Customers about CMC/Talisma policies on acceptable use of information resources.
b. Assuring that CMC/Talisma application and development personnel comply with this Acceptable Use Policy.
c. Using reasonable efforts to assist so that the CampusNet Service/CMC SaaS/Talisma SaaS information resources are not used in violation of this Acceptable Use Policy or for illegal unacceptable purposes through various directives, enforcement actions, and if necessary, suspension of user privileges.

Customer Liaison.
Customer Liaison, a Customer employee, is charged with the responsibility of ensuring that all Customer users of the CampusNet Service/CMC SaaS/Talisma SaaS:

a. Are informed of CMC CampusNet Service/CMC SaaS/Talisma SaaS policies on acceptable use of information resources.
b. Comply with these policies and procedures.
c. Use reasonable efforts to assist so that the CampusNet Service/CMC SaaS/Talisma SaaS information resources are not used in violation of this Acceptable Use Policy or for illegal or unacceptable purposes through various directives, enforcement actions, and if necessary, suspension of user privileges.

System Administrators.
System Administrators, each a CMC/Talisma employee, shall be responsible for the following:

a. Monitoring systems for misuse.
b. Promptly reporting in writing to the Privacy Officer, CampusNet/SaaS Executive, and Customer Liaison, as applicable, suspicion or occurrence of any unauthorized activity. The CampusNet/SaaS Executive, in concert with Customer Liaison, will decide next steps to ensure acceptable use.

All Personnel.
All personnel using or accessing the CampusNet Service/CMC SaaS/Talisma SaaS, whether employed or contracted with CMC/Talisma or by Customer, shall be responsible for the following:

a. Abiding by these CampusNet Service/CMC SaaS/Talisma SaaS Acceptable Use Policies.
b. Promptly reporting in writing to the Privacy Officer, CampusNet/SaaS Executive, and Customer Liaison, as applicable, suspicion or occurrence of any unauthorized activity.
c. Immediately reporting any known use by others of their accounts, logon IDs, passwords, PINs, and tokens.

Auditing and Compliance.
CMC/Talisma owns all CampusNet Service/CMC SaaS/Talisma SaaS information resources; use of such resources constitutes consent for CMC/Talisma to monitor, inspect, audit, collect, and remove any information without permission or further notice.

Training.
All Customer personnel (including contractors) using the CampusNet Service/CMC SaaS/Talisma SaaS shall be trained by Customer in what use is acceptable and what is prohibited by providing them the CMC/Talisma Acceptable Use Policy as described in this Policy. Any infraction of the CampusNet Service/CMC SaaS/Talisma SaaS Acceptable Use Policies shall constitute a security violation. Personnel may be held personally accountable and may be subject to disciplinary action, termination or employment and/or criminal prosecution.

Updates and Posting.
CMC/Talisma reserves the right to change or modify its Acceptable Use Policy at any time. When changed, the Customer Liaison will be advised and ensure distribution of the changed policy within Customer organization. Any such changes shall not materially adversely affect Customer's business or operations.

Hardware and Software Provisions

Acquiring Hardware and Software.
To prevent the introduction of malicious code and protect the integrity of the CampusNet Service/CMC SaaS/Talisma SaaS information resources, only CMC/Talisma and its Contractors will be permitted to provide hardware and software used at the CampusNet Service/CMC SaaS/Talisma SaaS facilities.

Complying with Copyright and Licensing.
All software used on CampusNet Service/CMC SaaS/Talisma SaaS information resources shall be subject to applicable licenses, as well as limitations and procedures identified in the Agreement. All Customer and CMC/Talisma personnel shall abide by intellectual property laws, including, without limitation, software copyright laws, and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

Using Personally Owned Software.
To protect the integrity of the CampusNet Service/CMC SaaS/Talisma SaaS information resources, Customer Data, CMC/Talisma and Customer personnel shall not use personally owned software on CampusNet Service/CMC SaaS/Talisma SaaS information resources. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally-owned or controlled software.

No Internet Privacy Expected.

Customer, and its authorized parties (including, without limitation, employees, contractors, subcontractors and business partners), acknowledge that Internet activities, if any, may be monitored for any legitimate business purpose, and all personnel accessing the Internet shall have no expectation of privacy.

Generally Prohibited Uses of Information Resources.

Generally prohibited activities when using the CampusNet Service/CMC SaaS/Talisma SaaS information resources shall include, but are not limited to, the following:

a. Stealing or copying of electronic files without permission, or posting or sending sensitive information outside of Customer or CMC/Talisma without management authorization.
b. Violating copyright laws, or any activities in violation, or reasonably likely to result in violation, of any applicable law, rule or regulation, or otherwise reasonably determined by CMC/Talisma or Customer to cause, or likely to cause, damage to CMC's/Talisma's or Customer's, or any of CMC/Talisma customer's or third party's hardware, software, or data.
c. Browsing the private files or accounts of others, except as provided by appropriate authority.
d. Performing unofficial activities that may degrade the performance of systems, such as the playing of electronic games or receiving large media files.
e. Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.
f. Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any CampusNet Service/CMC SaaS/Talisma SaaS computer, network, or information.
g. Accessing the CampusNet Service/CMC SaaS/Talisma SaaS without the approval of CampusNet Service/CMC SaaS/Talisma SaaS management.
h. Promoting or maintaining a private business, or using CampusNet Service/CMC SaaS/Talisma SaaS information resources for personal gain.
i. Sharing or using someone else's logon ID and password.
j. Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any Customer, CampusNet Service/CMC SaaS/Talisma SaaS or non-CampusNet Service/CMC SaaS/Talisma SaaS computer.
k. Conducting political fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.
l. Disclosing any Customer or CampusNet Service/CMC SaaS/Talisma SaaS information that is not otherwise public.
m. Performing any act that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, CMC/Talisma, Customer, or any person.

Security Testing Policy

CMC/Talisma hosted environments are built with firewalls and other security features, and attempts to obtain unauthorized access may result in prevention of access or other preventative steps taken to protect the integrity of the system. Customer and its representatives must adhere to the policies in place for hosted customers, including, without limitation, using appropriate security controls with individual credentials and access. Customer may not provide to third parties access via login or other access instructions that are provided for its own internal use. Violation of CMC/Talisma policy by Customer or its consultant, including but not limited to disruption of the system or that of any of other CMC/Talisma customers (for example, impact of customers in the shared hosting center by affecting their usage, performance, data, etc.) is prohibited and Customer and its consultant may be held fully responsible. If CMC/Talisma, Customer or its consultant determines that the activities of Customer or its consultant are impacting other customers, Customer and its consultant shall immediately stop the activities. This policy shall not be construed in any manner as a CMC/Talisma consent or waiver of rights. CMC/Talisma retains all rights to pursue recourse, including, without limitation, compensation for CMC/Talisma Time & Materials expended, and for CMC's/Talisma's defense and payment of any customer and/or third party claims, arising from Customer's or its consultant's acts or omissions.

CAMPUSNET[SM] SERVICE, CMC SAAS, AND TALISMA SAAS
E-MAIL POLICY

NOTE: This policy applies to the extent Customer uses e-mail applications through the CampusNet Service/CMC SaaS/Talisma SaaS.
CampusNet Service/CMC SaaS/Talisma SaaS e-mail facilities shall be used in an approved, ethical, and lawful manner to avoid loss or damage to the CampusNet Service/CMC SaaS/Talisma SaaS, or Customer operations, image, or financial interests and to comply with acceptable use of email policies outlined herein. All terms of the CampusNet Service/CMC SaaS/Talisma SaaS Acceptable Use Policy are incorporated herein by reference.

CampusNet Service/CMC SaaS/Talisma SaaS users on both Customer and CMC/Talisma side are required to notify CMC's/Talisma's CampusNet/SaaS Executive and Privacy Officer before engaging in any activities not clearly addressed in this E-mail Use Policy.

Electronic Mail and Messaging

Access to the CampusNet Service/CMC SaaS/Talisma SaaS electronic mail (e-mail) system and/or CampusNet Service/CMC SaaS/Talisma SaaS supplied Exchange™ services, is provided to Customer personnel whose duties require it for the conduct of Customer business over the CampusNet Service/CMC SaaS/Talisma SaaS. Since e-mail may be monitored for legitimate business purposes, all personnel using CampusNet Service/CMC SaaS/Talisma SaaS resources for the transmission or receipt of e-mail shall have no expectation of privacy.

Acceptable Use

The CampusNet Service/CMC SaaS/Talisma SaaS provides e-mail to facilitate the conduct of Customer's business via the CampusNet Service/CMC SaaS/Talisma SaaS. Occasional and incidental personal e-mail use shall be permitted if it does not interfere with either Customer or CMC's/Talisma's ability to perform its mission and meets the conditions outlined in official CampusNet Service/CMC SaaS/Talisma SaaS directives. However, while they remain in the system, personal messages shall be considered to be in the possession and control of CMC's/Talisma's CampusNet Service/CMC SaaS/Talisma SaaS.

Prohibited Use

Prohibited activities when using CampusNet Service/CMC SaaS/Talisma SaaS e-mail shall include, but not be limited to, sending or arranging to receive the following:

a. Information that violates state or federal laws, or CampusNet Service/CMC SaaS/Talisma SaaS regulations.
b. Unsolicited commercial announcements or advertising material, unless approved by management in advance.
c. Any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, CMC/Talisma, the recipient, the sender, or any other person.
d. Pornographic, racist or offensive material, chain letters, unauthorized mass mailings, or malicious code.
e. Messages that use an alias sender in a malicious or misleading manner ("spoofing"), or for distribution of any virus, Trojan horse or other deleterious routines, or in connection with a distributed denial of service attacks.

Encryption

Encrypting e-mails or messages shall comply with the following:

a. Use encryption software and the methods approved by official CampusNet Service/CMC SaaS/Talisma SaaS sources.
b. Place the key or other similar file for all encrypted e-mail in a directory or file system that can be accessed by management personnel prior to encrypting email.
c. Supply the key or other device needed to decrypt the e-mail upon request by authorized CampusNet Service/CMC SaaS/Talisma SaaS management.

Authorized Monitoring

System administrators and other personnel with unrestricted access to email and similar services shall receive management approval prior to decrypting or reading the e-mail traffic of other personnel. If management approval is not immediately available, then system administrators and other personnel that intercept, read, or restrict e-mail accounts shall document their actions and provide that documentation to management personnel within twenty-four (24) hours.

CAMPUSNET[SM] SERVICE, CMC SAAS, AND TALISMA SAAS

ANTI-SPAM POLICY

CMC/Talisma offers certain software offerings which could be utilized to send bulk "spam" email messages; however CMC/Talisma does not condone or permit use of the CampusNet Service/CMC SaaS/Talisma SaaS to deliver unsolicited, bulk e-mail ("Spam"). In order to preserve e-mail as a powerful business and personal communication tool, and to better serve and protect the privacy of its customer and their subscribers, CMC/Talisma has established this Anti-Spam Policy to ensure that subscribers have a reasonable expectation of receiving the mail that is sent through use of the CMC's/Talisma's email services. If Customer has or at some point purchases this portion of CMC's/Talisma's software offering, Customer agrees to abide by the following policy at all times:

1. Standards for Delivery. CMC/Talisma will not deliver e-mail to a subscriber who would not have a reasonable expectation of receiving the e-mail from Customer, determined as follows:

   1.1 Direct Request. If the subscriber provided its e-mail address directly to Customer in order to receive the e-mail to be sent, CMC/Talisma will send the e-mail. If the subscriber did not provide its e-mail address to Customer for such purpose, the content relevance of the e-mail must be addressed, as set forth below, to determine whether the subscriber could reasonably expect to receive the e-mail.

   1.2 Content Relevance. If the content of the mailing relates to subject matter about which the subscriber previously requested information, the subscriber will be deemed to have a reasonable expectation of receiving the e-mail, and CMC/Talisma will include the subscriber in Customer's initial mailing, provided that (i) the subscriber is given the ability either to opt-in or opt-out of the mailing list for future mailings, as described below, and (ii) the mailing clearly informs the subscriber of its option to subscribe or unsubscribe to the list.

   • Opt-Out Mailing. With respect to subscribers who have had a previous relationship with Customer, the mailing may be sent via an opt-out approach, whereby the subscriber will remain on the mailing list unless the subscriber requests to be removed.
   • Opt-In Mailing. With respect to subscribers who have not had a previous relationship with Customer, the mailing must be sent via an opt-in approach, whereby those subscribers who wish to subscribe must request to be added to the mailing list. An opt-in mailing may be either a one-time mailing announcing the offer or a multiple issue trial mailing of reasonable duration.

If the content of the mailing relates to subject matter about which the subscriber had not previously requested information, CMC/Talisma will not send Customer's proposed mailing until Customer demonstrates that it has taken measures which allow subscribers to either participate in the mailing or not participate in the mailing, at their option.

2. Additional Precautions.

   2.1 CMC/Talisma expressly prohibits (i) delivery of chain letters, whether or not subscribers wish to receive such letters, (ii) malicious mailings, including but not limited to flooding a subscriber or site with very large or numerous pieces of e-mail, (iii) forging of header information (the practice of making it appear as though an e-mail message originated from another source) or intentionally misleading subject lines, and (iv) delivery of e-mail advertising illicit or illegal activities.

   2.2 In the event the source of a list or the expectations of some or all of the users on a particular list is unclear, or the duration of the time between when the addresses were collected and the first e-mail is to be sent could cause confusion, clarity must be provided in the form of a preamble in each of the first two e-mails sent. The preamble must explain whom the e-mail is from, the reason the person is receiving the message, the possible source of the e-mail address (i.e., ways in which the sender may have obtained the address) and clear instructions on how to unsubscribe.

   2.3 If Customer supplies CMC/Talisma with a new list to be added to the system or new subscribers to be added to an existing list, Customer will be required to represent and warrant that the new names adhere to CMC's/Talisma's policy regarding the source of names.

   2.4 In addition to the foregoing, Customer must take all reasonable steps necessary to ensure that subscribers added to Customer's mailing lists have a clear expectation of receiving the mail that Customer plans to send, which efforts shall include, but shall not be limited to, notifying subscribers of the content of the proposed mailings.

3. Reservation of Rights. CMC/Talisma reserves the right at any time to implement technical mechanisms to prevent activities that violate the policies set forth in this Policy, to refuse to send e-mail that does not meet the aforementioned requirements. CMC/Talisma reserves all legal and equitable rights in enforcing this policy.