REGOLAMENTO PER I SERVIZI INFORMATICI.

REGOLAMENTO RETE DI ATENEO

1. **Rete di Ateneo**

   1.1 La Rete di Ateneo è costituita dall'insieme di tutte le Reti Locali delle Strutture dell'Ateneo (RLS), interconnesse tramite Dorsali di Rete (DRA), finalizzata a condividere risorse informatiche comuni e a permettere l'interscambio di informazioni ed ogni altra applicazione telematica all'interno e all'esterno dell'Ateneo.

   1.2 E' compito dell'Ateneo assicurare l'infrastruttura di rete per l'interconnessione tra le Strutture e con l'esterno. La Rete di Ateneo è interconnessa alla rete GARR e, tramite quest'ultima, alla rete Internet. Le norme che regolano la rete GARR sono parte integrante del presente regolamento.

   1.3 Ogni utente della Rete di Ateneo è tenuto al rispetto delle "Norme di buon uso dei servizi di rete".

2. **Organi di gestione e controllo**

   2.1 La progettazione delle infrastrutture fisiche e tecnologiche è demandata al Centro per l'Informatica (CPI).

   2.2 Il CPI è la struttura preposta alla gestione tecnica, al controllo ed alla manutenzione delle infrastrutture che costituiscono la Rete di Ateneo.

3. **Infrastruttura fisica**

   3.1 La progettazione del cablaggio di nuovi edifici o di edifici in via di ristrutturazione deve prevedere la connessione in rete locale di ogni postazione telematica di lavoro o di studio. All'uopo, l'Amministrazione Centrale dell'Ateneo dovrà finanziare sia le opere di cablaggio, incluse eventuali opere edili, che l'acquisto delle relative apparecchiature di rete.

   3.2 Le Strutture possono successivamente procedere, a proprie spese, all'ampliamento o modifica del cablaggio delle proprie RLS, purché nel rispetto delle norme riportate al punto 3.3. Nel caso l'ampliamento comporti l'installazione di ulteriori apparati di rete, questi ultimi saranno acquistati dall'Amministrazione Centrale, compatibilmente con le risorse finanziarie disponibili.

   3.3 Le Strutture che intendono procedere a proprie spese a nuove installazioni di apparati di rete o a modifiche delle proprie RLS, dovranno preventivamente farne richiesta al CPI.

4. **Interconnessione delle RLS alla Rete di Ateneo e ad Internet**

   4.1 Nessuna Struttura può attivare connessioni autonome delle proprie Reti Locali con quelle di altre Strutture, se non concordate ed approvate preventivamente dal CPI.

   4.2 La connessione tra Enti esterni e la rete di Ateneo va valutata caso per caso, dal Rettore ed approvata dagli Organi Accademici sia in relazione alle finalità istituzionali dell'Ente che alle sue affiliazioni a livello nazionale.

5. **Protocolli supportati**

   5.1 Nella Rete di Ateneo viene garantito il supporto della famiglia di protocolli TCP/IP.

   5.2 Prima di inserire un qualunque dispositivo (elaboratore, apparato, periferica) in rete è necessaria, da parte del responsabile del dispositivo stesso, inoltrare una richiesta al CPI, che provvederà all'assegnazione dell'indirizzo IP e ad effettuarne la registrazione nel dominio **unistrasi.it.**

NORME DI "BUON USO" DEI SERVIZI DI RETE.

L'utilizzo delle tecnologie informatiche sta assumendo un ruolo sempre più importante nell'ambito della ricerca, della didattica e dell'amministrazione di questo Ateneo. Gli utenti delle risorse informatiche dell'Università hanno la responsabilità di non abusarne e di rispettare i diritti degli altri membri della comunità accademica. Queste norme stabiliscono le linee guida per un buon uso delle risorse informatiche, nello spirito dell'RFC 1855 (Request for Comment 1855- **"Netiquette Guidelines"**) e delle direttive emanate dal Gruppo Armonizzazione Reti della Ricerca **(GARR)** (il servizio telematico che connette tra loro le Entità della Ricerca Scientifica Italiana).

1. Definizioni

Rete di Ateneo: l'insieme di tutte le reti locali delle strutture dell'Ateneo, allo scopo di condividere risorse informatiche comuni e di permettere l'interscambio di informazioni e di ogni altra applicazione telematica all'interno e all'esterno dell'Ateneo.

Sistema in Rete: ogni computer, terminale, stampante o rete locale connessi alla Rete d'Ateneo.

CPI: Centro per l'Informatica. E' la struttura cui è affidata la gestione tecnica, il controllo e al manutenzione della Rete di Ateneo.

Utente: qualsiasi persona, autorizzata o meno, che utilizzi un Sistema in Rete.

2. Scopo

Lo scopo di queste Norme è quello di garantire un'infrastruttura di rete che faciliti la ricerca, la didattica, l'amministrazione e le altre attività istituzionali dell'Ateneo.

In particolare, queste Norme mirano a promuovere i seguenti obiettivi:

A. Assicurare l'integrità, l'affidabilità, la disponibilità e l'alto livello di performance dei Sistemi in Rete;
B. Assicurare che i Sistemi siano effettivamente utilizzati per gli scopi previsti dall'Ateneo;
C. Stabilire le sanzioni per i trasgressori.

3. Campo d'applicazione

Queste Norme riguardano tutti gli Utenti dei Sistemi in Rete; si applicano all'uso di tutti i Sistemi presenti nella Rete di Ateneo.

4. Uso appropriato dei Sistemi in Rete

Queste Norme stabiliscono dei criteri generali per un corretto uso dei Sistemi in Rete. Le singole strutture universitarie (Facoltà, Dipartimenti, Laboratori, Centri, ecc.) possono stabilire regolamenti più specifici riguardo alle politiche d'uso dei Sistemi che amministrano. In caso di conflitto tra vari regolamenti, prevalgono le presenti Norme.

A. **Uso appropriato.** I Sistemi in Rete possono essere utilizzati esclusivamente per gli scopi autorizzati, vale a dire come supporto alla ricerca scientifica, alla didattica, all'amministrazione universitaria e alle altre funzioni proprie di quest'Ateneo.

B. **Autorizzazioni.** Gli Utenti hanno diritto ad accedere solo a quei servizi di Rete per i quali sono stati espressamente autorizzati.

C. **Divieti specifici.** Le seguenti categorie d'uso sono improprie e proibite:

C.1. Utilizzo che impedisca, interferisca, o causi in ogni modo danno alle attività degli altri utenti. Gli Utenti non debbono impedire o interferire o tentare di impedire o interferire in qualsiasi forma con i servizi offerti agli altri Utenti. In questa categoria rientrano il "resource hogging" (allocazione esaustiva di una risorsa, tale da non consentirne l'utilizzo ad altri utenti.), l'uso improprio di mailing list, la propagazione delle "chain letters" (le cosiddette "Catene di S. Antonio", messaggi di Posta Elettronica, generalmente contenenti informazioni inesatte, inviati con richiesta di diffusione ad altre persone) e dei "virus hoaxes" (comunicazione riguardante la presenza di un nuovo virus, in realtà del tutto inesistente, accompagnato generalmente da una preghiera di massima diffusione (v. "chain letters"), lo "spamming" (messaggi pubblicitari o

comunicazioni che non siano stati sollecitati in modo esplicito) ed il "bombing" (invio ripetuto di messaggi verso un indirizzo di posta elettronica allo scopo di bloccarne l'accesso). Sono inoltre proibiti tutti i comportamenti che generano un eccessivo traffico di rete.

C.2. Incompatibilità con lo status non-profit dell'Ateneo. L'Università per Stranieri di Siena è un ente non-profit e come tale è soggetta a leggi specifiche riguardanti regime fiscale, attività politiche, uso dei beni e altre questioni analoghe. Pertanto l'utilizzo a scopi commerciali dei Sistemi in Rete è generalmente proibito, eccetto nei casi specificatamente autorizzati dagli organi competenti. Il divieto non comprende lo scambio d'informazioni commerciali, anche con enti esterni, relative alle attività istituzionali dell'Ateneo. E' inoltre proibito l'uso dei Sistemi in Rete per propaganda politica o elettorale.

C.3 Molestie sessuali e minacce. Gli Utenti non possono utilizzare i Sistemi in Rete allo scopo di molestare, minacciare o inviare messaggi non graditi.

C.4. Danneggiamento dei Sistemi in Rete dell'Ateneo o di altre organizzazioni. In questa categoria rientrano tra l'altro i seguenti sei punti:

C.4.1. Tentativi di violazione dei sistemi. Gli Utenti non devono violare o tentare di violare i sistemi di sicurezza informatici.

C.4.2. Accesso e uso non autorizzato. L'Università riconosce l'importanza di preservare la privacy degli Utenti e dei dati immagazzinati nei Sistemi in Rete. A tal fine gli Utenti non devono né cercare di ottenere accessi non autorizzati, né favorire analoghe attività da parte di altri Utenti, interni o esterni. Ad esempio, organizzazioni esterne all'Ateneo o singoli individui non possono utilizzare senza una specifica autorizzazione i Sistemi in Rete, eccetto per quanto riguarda i servizi di pubblico dominio (p.e.: consultazione del Servizio Bibliotecario, del server web,…). Inoltre gli Utenti non possono, deliberatamente e in modo non autorizzato, modificare o tentare di modificare dati contenuti nei Sistemi in Rete. Gli Utenti non possono intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete d'Ateneo, che non siano loro diretti.

C.4.3. Uso camuffato. Gli utenti non possono mascherare la loro identità quando usano i Sistemi in Rete, eccetto nei casi in cui l'accesso anonimo è esplicitamente autorizzato. Gli Utenti non possono inoltre impersonare altri individui o usare false identità.

C.4.4. Distribuzione di virus informatici. Gli Utenti non devono né distribuire coscientemente né lanciare virus o altri programmi similari.

C.4.5. Modifica o rimozione di dati o apparecchiature. Gli Utenti non possono, a meno di specifiche autorizzazioni, rimuovere o modificare alcun dato o apparecchiatura appartenente alla Rete d'Ateneo.

C.4.6. Uso non autorizzato di dispositivi. Gli Utenti non possono, a meno di specifiche autorizzazioni, connettere fisicamente o elettricamente, alcun dispositivo esterno (dischi, modem, stampanti…) ai Sistemi in Rete.

C.5. Violazione di leggi vigenti. L'uso di Sistemi in Rete in violazione di norme del Codice Civile o Penale è proibito. Esempi di queste violazioni sono: divulgazione di schemi piramidali (noti anche come "Ponzi Scheme", sono truffe usate per ottenere profitti illeciti, promettendo ad ogni investitore (membro dello schema) la concessione di tassi di rendimento elevatissimi. I

rendimenti vengono però ottenuti solo grazie al reclutamento a catena (o meglio, in forma piramidale) di nuovi investitori; distribuzione di materiale osceno; ricezione, trasmissione o possesso d'immagini pornografiche relative a minori; violazione di copyright.

C.6. Violazione di contratti universitari. L'utilizzo dei Sistemi in Rete deve essere compatibile con gli obblighi contrattualmente assunti dall'Ateneo, particolarmente in materia di licenze d'uso di risorse informatiche.

C.7. Violazione di norme relative a Reti Trasmissione Dati esterne all'Ateneo. Nel caso un Utente acceda a Reti Trasmissione Dati esterne all'Ateneo, è tenuto ad osservare le norme stabilite dagli amministratori delle suddette Reti.

C.8 Responsabilità connesse ai codici d'accesso personali. Gli Utenti sono responsabili del mantenimento della sicurezza dei codici e delle password loro assegnate. Codici e password sono normalmente assegnati a singoli utenti, di conseguenza non devono essere condivisi con altre persone senza autorizzazione da parte dell'Amministratore del Sistema. Gli Utenti sono responsabili per ogni attività connessa all'utilizzo dei codici e delle password loro assegnate.

C.9. Responsabilità dei contenuti. Ogni struttura universitaria che pubblichi documenti in forma elettronica accessibili attraverso i Sistemi in Rete, è responsabile dei contenuti.

5. Accesso a dati personali

L'Università per Stranieri di Siena riconosce il diritto alla privacy relativo ai dati personali presenti nei Sistemi in Rete. Ciò nonostante possono verificarsi circostanze nelle quali l'amministratore di sistema, secondo quanto stabilito dalla Legge 675, ha il diritto di accedere ai dati personali anche in assenza del consenso dell'Utente.

A. Condizioni. L'amministratore di sistema può accedere ai dati personali senza il consenso dell'Utente qualora si presenti una delle seguenti circostanze:

A.1 nel caso in cui sia necessario identificare o diagnosticare problemi o vulnerabilità presenti nel sistema al fine di preservarne l'integrità;
A.2 su richiesta delle autorità giudiziarie;
A.3 quando abbia ragionevoli dubbi sull'avvenuta violazione delle presenti Norme e ritenga che il monitoraggio dei dati possa essere d'aiuto nell'individuazione dei responsabili.

B. Autorizzazioni. In accordo con il diritto alla privacy dell'Utente, l'accesso ai dati personali può in ogni caso avvenire solo con il consenso del Rettore oppure del Direttore Amministrativo nel caso l'Utente appartenga al personale Tecnico-Amministrativo dell'Ateneo. L'amministratore di sistema ha in ogni caso la facoltà di conservare traccia dell'attività relativa all'uso dei servizi di rete senza alcun consenso.

C. Disattivazione del codice personale. L'amministratore di sistema può disattivare un codice d'accesso personale, nel caso in cui l'Utente sia sospettato di violazione delle presenti Norme o quando si renda necessario al fine di preservare l'integrità del Sistema in Rete. L'Utente riceverà, qualora possibile, una notifica preventiva della disattivazione.

D. Uso di sistemi di monitoraggio. Nell'atto della connessione di un elaboratore alla Rete d'Ateneo, l'Utente autorizza automaticamente l'amministratore di Rete ad utilizzare sistemi in grado di verificarne il livello di sicurezza nonché il relativo traffico.

E. Archiviazione delle attività di rete. Gran parte dei Sistemi in Rete è in grado di produrre archivi contenenti elenchi descrittivi relativi alle risorse di rete utilizzate dai singoli Utenti, i cosiddetti file di log. Questi archivi sono usati per facilitare il recupero dei dati in caso di malfunzionamento oppure a fini di gestione di Sistema. Ogni amministratore di sistema può

stabilire le proprie politiche di gestione dei file di log e la tipologia delle informazioni personali in essi contenute.

6. Procedure disciplinari

Gli utenti sono tenuti a segnalare tempestivamente al CPI ogni violazione o sospetta violazione delle presenti Norme.

Nel caso vi sia la certezza di una violazione delle presenti Norme, l'Utente in causa è soggetto a restrizioni temporanee o permanenti dei propri privilegi d'accesso alla Rete d'Ateneo.

Inoltre qualora vi siano violazioni delle leggi vigenti, l'Utente sarà perseguibile da parte delle Autorità Giudiziarie.

Le disposizioni del regolamento e le norme di buon uso hanno immediata vigenza.