REGOLAMENTO PER L'UTILIZZO DI COMPUTER E RETI DI TRASMISSIONE DATI

Art. 1 – OGGETTO E FINALITÀ

1. Il presente Regolamento fornisce le linee guida principali e le regole per un corretto uso delle infrastrutture e delle risorse informatiche dell'Università Ca' Foscari di Venezia, d'ora in avanti denominata "*Università*" o "*Ateneo*".
2. Gli elaboratori e la rete di trasmissione dati costituiscono strumenti indispensabili per l'Università, in quanto consentono l'accesso, l'elaborazione e la distribuzione dell'informazione e della conoscenza sviluppate all'interno ed all'esterno di essa. L'Università pertanto concede in uso ai docenti, al personale tecnico amministrativo, ai collaboratori ed esperti linguistici, nonché agli studenti le proprie apparecchiature informatiche e ne promuove l'utilizzo, ritenendole strategiche per le attività didattiche, scientifiche ed amministrative.
3. Poiché tali tecnologie potenziano la capacità individuale all'accesso, alla copia, all'analisi ed alla rielaborazione delle informazioni, gli utenti devono comunque essere coscienti dei limiti che ne configurano un uso appropriato, in particolare per quanto riguarda il rispetto degli altrui diritti alla privacy, della proprietà intellettuale e degli altri diritti ed obblighi conseguenti.
4. Gli utenti della rete e delle risorse di elaborazione dell'Università sono tenuti a farne uso corretto, ad averne cura ed a rispettare i diritti sopra citati, osservando nello specifico le regole stabilite nel presente Regolamento.
5. L'Ateneo si impegna a dimensionare opportunamente le risorse informatiche e di rete disponibili in funzione delle necessità e priorità dell'utenza.

Art. 2 - SINTESI DEGLI OBBLIGHI FONDAMENTALI

1. Gli utenti delle risorse informatiche dell'Ateneo, nel rispetto delle leggi e normative vigenti, devono porre particolare attenzione a:
    a. utilizzare le risorse con modalità orientate alle finalità dell'istituzione universitaria;

b. evitare accessi non autorizzati alle risorse;
c. evitare di abusare delle risorse comuni, monopolizzandone l'uso o limitandone la disponibilità agli altri utenti;
d. rispettare i diritti d'autore ed il copyright, le licenze d'uso e l'integrità di risorse informative basate su computer;
e. rispettare in generale i diritti degli altri utenti di risorse informatiche;
f. rispettare i regolamenti di Enti e Strutture che interagiscono con l'Ateneo.
g. responsabilità delle strutture e dei singoli utenti ed è revocabile con provvedimento motivato.

2. La concessione in uso delle risorse informatiche dell'Ateneo implica specifiche

Art. 3 - AMBITO ED APPLICABILITÀ DEL REGOLAMENTO

Il presente Regolamento si applica a tutti gli studenti, al personale docente, al personale tecnico-amministrativo, ai collaboratori ed esperti linguistici dell'Università, ai dottorandi di ricerca, ai titolari di borse post-dottorato, agli esterni che operano per conto dell'Ateneo ed in generale a tutti coloro a cui a qualsiasi titolo sia concesso l'uso delle risorse informatiche dell'Università, sia controllate individualmente che condivise, gestite su un singolo computer o rese disponibili in rete. Si applica a tutte le attrezzature di elaborazione e comunicazione possedute o detenute a qualsiasi titolo dall'Ateneo.

Art. 4 - INTEGRAZIONE CON ALTRE NORMATIVE

All'interno dell'Ateneo sono presenti strutture e comunità dotate di specifica autonomia. Inoltre l'Università non è isolata da altre comunità ed autorità esterne e dai loro regolamenti e/o dalle loro leggi. L'integrazione del presente Regolamento con altre normative è basata sulle seguenti assunzioni:

a) specifiche strutture dell'Ateneo (ad es. Dipartimenti o Centri) possono definire condizioni d'uso particolari per le risorse informatiche sotto il proprio controllo. Tali condizioni devono essere coerenti con il presente Regolamento senza costituirne deroga, ma possono fornire ulteriori dettagli, linee guida e/o restrizioni. Le strutture dovranno

curare la pubblicizzazione dei regolamenti locali in questione e delle norme riguardanti l'uso autorizzato ed appropriato degli apparati per cui sono responsabili.

b) A livello nazionale ed internazionale esistono comunità informatiche cui l'Università aderisce per fini istituzionali di ricerca e di didattica, e con cui interagisce prevalentemente tramite le reti informatiche. Tali comunità hanno definito norme e regolamenti per l'utilizzo delle risorse messe in comune. L'Università è quindi tenuta ad adeguare le proprie attività ed azioni alle norme suddette. Di particolare rilievo risulta il rapporto con la comunità di rete scientifica e di ricerca italiana, rappresentata dall'ente denominato GARR (Gruppo Armonizzazione Reti di Ricerca italiano), ed il rispetto delle regole (*Acceptable User Policy*) da tale ente definite. Gli utenti dell'Ateneo devono conformarsi alle normative suddette.

c) Le leggi dello Stato, se difformi, prevalgono sul presente Regolamento e sulle norme specifiche citate nei punti precedenti.

Art. 5 - NORME

1. **Integrità delle risorse informatiche** - Gli utenti di computer devono rispettare l'integrità delle risorse informatiche, secondo quanto di seguito precisato:
    a. **inserimento, rimozione o modifica di apparati di rete –** Gli utenti non devono inserire, modificare o rimuovere apparati in rete senza preventiva autorizzazione degli amministratori di rete;
    b. **abusi nell'utilizzo di risorse informatiche** – Gli utenti non devono abusare delle risorse informatiche dell'Università, alterandole o facendone cattivo uso. Ciò include, a mero titolo esemplificativo:
        - tentativi intenzionali di accedere o apportare modifiche ad informazioni personali, individuali o ogni altra informazione dell'Università per cui l'utente non possieda idonea autorizzazione;
        - tentativi intenzionali di apportare modifiche a sistemi o

altre risorse informatiche per cui l'utente non possieda idonea autorizzazione;

- invio intensivo di posta elettronica indesiderata o invasiva (*spam*);
- stampa di copie cartacee per fini non istituzionali di documenti, files, dati o programmi;
- modifiche di configurazioni di sistemi di uso collettivo che non siano state autorizzate dagli amministratori di sistema (cfr. art 7) o che violino copyright esistenti;
- tentativi intenzionali di bloccare o mandare fuori servizio computer, reti, servizi od altre risorse informatiche dell'Ateneo;
- più in generale, attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti;
- danneggiamento o vandalismo nei confronti di attrezzature di calcolo, apparati, software, files od altre risorse informatiche;

c. **programmi nocivi** - Gli utenti devono assicurarsi e garantire di non sviluppare od usare programmi od utilità che interferiscano con l'attività di altri utenti, o che modifichino parti del sistema o che accedano ad informazioni private o riservate. L'uso di ogni programma nocivo espone ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte dell'Università;

d. **Gestione dei dispositivi di elaborazione personali** - Gli utenti sono tenuti ad applicare ai dispositivi di elaborazione personali, di cui hanno disponibilità, le cure necessarie per una corretta manutenzione, includendo tra queste:

- attivazione del controllo d'accesso al dispositivo mediante autenticazione (username e password);

- installazione e manutenzione in efficienza dei sistemi antivirus;
- attuazione di backup sistematici;
- verifiche di sicurezza relative all'immissione in rete.

2. **Accesso non autorizzato**:
   Gli utenti di risorse informatiche dell'Ateneo non devono accedere a computer, software, dati, informazioni o reti senza appropriata autorizzazione, o abilitare intenzionalmente altri all'accesso non autorizzato, indipendentemente dal fatto che le risorse citate appartengano o meno all'Ateneo.
   Un utente che sia stato autorizzato ad utilizzare un *account* protetto tramite *password* o altra tecnologia è tenuto a custodire con cura ed a mantenere riservate le chiavi d'accesso relative all'*account*. L'utente è personalmente soggetto a responsabilità civili e penali, in caso di abusi o incidenti di sicurezza, nel caso divulghi la *password* o renda accessibile ad altri l'*account* senza il permesso dell'amministratore di sistema. Ogni anomalia scoperta in *account* di sistema o relativa alla sicurezza di sistemi o reti deve essere segnalata tempestivamente all'amministratore di sistema preposto, in modo che possano essere attuati gli opportuni passi per investigare sui problemi e risolverli;
3. **Diritto d'autore, copyright e licenze d'uso -** Gli utenti di computer devono rispettare diritti d'autore, copyright e licenze d'uso di software, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge.
   a. **Copia** – Ogni materiale protetto da diritto d'autore o copyright non deve essere copiato al di fuori di quanto specificato dal proprietario dei diritti o del copyright o di quanto previsto dalle leggi sul diritto d'autore. Il materiale protetto non può essere copiato per mezzo di attrezzature o sistemi dell'Università, fatto salvo quanto conseguente alla disponibilità di una licenza d'uso valida, o permesso dalle leggi sul diritto d'autore e sul copyright.
   b. **Numero di utenti simultanei** – Il numero e la distribuzione delle copie di materiale soggetto a diritto d'autore o copyright deve essere gestito in modo che il numero di utenti simultanei in un dipartimento o struttura non superi il numero di copie originali

acquistate dal dipartimento/struttura, salvo quanto diversamente stipulato nel contratto di acquisto o permesso dalle leggi vigenti.

c. **Uso delle informazioni e dei materiali** – Tutte le informazioni soggette a diritto d'autore o copyright (testi, immagini, icone, programmi, video, audio, etc.) ottenute da computer o risorse di rete devono essere usate in conformità con le leggi vigenti. L'origine del materiale copiato deve essere correttamente attribuita ed evidenziata. Il plagio di informazioni digitali è soggetto alle stesse sanzioni che si applicano al plagio di altre opere o tipologie di dati.

Art. 6 - ATTIVITÀ ESPRESSAMENTE PROIBITE

1. È proibito l'uso di computer, reti, attrezzature o servizi di comunicazione elettronica (quali posta elettronica, *instant messaging* o similari) per inviare, visualizzare o scaricare messaggi che comportino dolo, frode, molestie di qualsiasi natura o altri messaggi o materiale che costituiscano violazioni delle leggi vigenti o dei regolamenti universitari.
2. *Mailing lists* - Gli utenti non devono violare gli statuti delle *mailing lists* elettroniche (inclusi i *news groups* locali e di rete ed i *bulletin-boards) e* sono tenuti a rispettarne le finalità.
3. Pubblicità - Le attrezzature di comunicazione elettronica dell'Ateneo non devono essere utilizzate per trasmettere pubblicità personale o commerciale.
4. Privacy – Sono proibite le violazioni della privacy così come sancito dal D.Lgs. n. 196/2003 "*Codice in materia di protezione dei dati personali*" contenente standard e regole che disciplinano il trattamento di dati personali e/o sensibili, relativi allo stato di salute personale o giudiziari.
5. Uso politico, religioso e commerciale:
    a. Uso politico o religioso - Le risorse informatiche dell'Università non devono essere utilizzate per finalità connesse all'attività di propaganda di partiti o organizzazioni religiose.

b. Uso commerciale – Le risorse informatiche dell'Ateneo non devono essere utilizzate per fini commerciali, salvo quando permesso da Regolamenti dell'Ateneo, o con l'approvazione di un funzionario dell'Ateneo titolato a rilasciare l'approvazione medesima.

Art. 7 - FIGURE E RESPONSABILITÀ DEGLI AMMINISTRATORI DELLE RISORSE INFORMATICHE

1. Il Titolare dell'Ateneo, identificato nella figura del Rettore, è responsabile di fronte alla legge di tutti i computer, gli apparati di rete e le reti acquistate od affittate dall'Università.

2. Il controllo e la supervisione di ogni particolare sistema è delegato al responsabile della specifica struttura dell'Università che lo ospiti e/o se ne faccia carico (ad es. Preside di Facoltà o Direttore di Dipartimento). Per attrezzature possedute o detenute dall'Università, tale soggetto è definito **amministratore responsabile** ai fini del presente Regolamento.

3. L'amministratore responsabile può delegare altre persone ad amministrare il sistema, definite **amministratori di sistema**.

Art. 8 - AMMINISTRAZIONE DI SISTEMA

1. L'attività dell'amministratore di sistema può inquadrarsi in due contesti complementari:
   a. **Attività di ordinaria amministrazione** - Volta a garantire il normale funzionamento e lo sviluppo dei sistemi amministrati. In tal caso l'amministratore di sistema opera di concerto con l'utente, e comunque coordinandosi in via preventiva con l'amministratore responsabile e con gli amministratori e responsabili di rete (cfr. art. 9);
   b. **Gestione delle emergenze** - Quando si rilevino condizioni che pongano a rischio immediato la corretta funzionalità dei sistemi o della rete, o la sicurezza dei dati e dei sistemi, l'amministratore di

sistema può operare in autonomia e per le vie brevi, qualora l'onere del coordinamento limiti l'efficacia e la tempestività degli interventi. Immediatamente dopo l'intervento, è tenuto comunque a segnalare per iscritto agli utenti coinvolti e agli amministratori responsabili di pertinenza i dettagli dell'evenienza occorsa.

2. L'amministratore di sistema deve avere ragionevole cura:
    a. nel prendere precauzioni contro i furti ed i danni ai componenti del sistema;
    b. nell'attuare rigorosamente tutti gli accordi di licenza hardware e software applicabili al sistema;
    c. nel trattare informazioni riguardanti gli utenti del sistema, nonché le informazioni depositate nel sistema dagli utenti medesimi, in modo appropriato, applicando rigorosamente le norme e le pratiche atte a garantire la sicurezza dei sistemi, delle reti e dei dati. Si fa particolare riferimento al caso di azioni dolose volte a violare l'integrità dei sistemi, dei dati o della privacy (ad es. intrusioni, diffusioni di virus, etc.), ed al caso di incidenti di natura tecnica (ad es. incendio, perdita di dati, etc.);
    d. nel diffondere informazioni sui regolamenti e le procedure specifiche che regolano l'accesso e l'uso del sistema, sui servizi forniti e su quelli esplicitamente non forniti. Un documento scritto consegnato agli utenti o messaggi inviati tramite il sistema stesso saranno considerati una notifica adeguata;
    e. nel collaborare con amministratori di altri computer o reti, interni od esterni all'Università, per trovare e correggere problemi causati ad altri dall'uso/abuso del proprio sistema.
3. Un amministratore di sistema può temporaneamente interdire l'accesso e l'uso delle risorse informatiche ad un utente se, sulla base di comprovati motivi, lo ritiene necessario per garantire la sicurezza del sistema o della rete. Se l'amministratore di sistema ha chiare evidenze di cattivo uso delle risorse informatiche che indirizzino ad attività di elaborazione o files di uno specifico individuo, deve attuare uno o più dei seguenti passi, considerati appropriati per la protezione degli altri utenti, della rete e dei sistemi di computer:
    a. notificare per iscritto le eventuali indagini ai responsabili tecnico

ed amministrativo di rete ed ai responsabili delle strutture coinvolte;

b. adottare tutti i provvedimenti e le azioni ritenute necessarie e/o opportune dai responsabili di cui al punto a), per inibire il propagarsi dei danni alle risorse di rete.

Art. 9 – RESPONSABILI DELLA RETE

1. A livello di Ateneo vengono definite le figure di **responsabile tecnico della rete** e di **responsabile amministrativo della rete**.

2. Il responsabile tecnico della rete svolge le funzioni:

   a. di amministratore della rete di Ateneo. Ha tutti gli obblighi e le mansioni di un amministratore di sistema ove si intenda come sistema la rete di Ateneo nella sua globalità;

   b. di referente tecnico verso le comunità di rete esterne, ed in particolare verso l'ente denominato GARR;

   c. di ispezione e sorveglianza. Il responsabile tecnico della rete può richiedere agli amministratori di sistema l'ispezione di apparati e sistemi di competenza dei medesimi, nell'ambito delle attività di monitoraggio e diagnosi dei problemi di rete.

3. Il responsabile amministrativo della rete svolge le funzioni:

   a. di amministratore responsabile della rete di Ateneo intesa nella sua globalità;

   b. di referente amministrativo verso le comunità di rete esterne, ed in particolare verso l'ente denominato GARR.

Art. 10 - SICUREZZA E VISIBILITA' DEI DATI

1. Gli utenti devono essere edotti del fatto che esistono limiti intrinseci nel

livello di sicurezza conseguibile nella protezione dei dati ospitati nei servers di uso collettivo e trasmessi dalle reti informatiche dell'Ateneo. Tali limiti sono connaturati con le tecnologie attualmente disponibili per i servers e per le reti.

2. In particolare, ciò vale per i più comuni servizi e protocolli tipicamente utilizzati in Internet quali l'accesso a pagine web o l'invio di posta elettronica, il cui livello di sicurezza è intrinsecamente basso e che possono essere soggetti a pratiche di monitoraggio o di intercettazione da parte di terzi.
3. L'Ateneo, tramite l'azione degli amministratori di rete e dei sistemi, pone in opera ed aggiorna costantemente le contromisure piu' opportune per ridurre i fattori di rischio. Va comunque ribadito che:
    - l'adozione di misure di sicurezza può avere un costo in termini di praticità e libertà d'utilizzo delle funzionalità di rete;
    - il rischio non può essere completamente azzerato e non può quindi essere data una garanzia di protezione totale dei dati.
4. Gli utenti devono inoltre essere resi edotti del fatto che:
    - in relazione alle mansioni loro attribuite, gli amministratori di rete o di sistema hanno accesso ai dati ospitati nei sistemi e trattati dalle reti di cui hanno la gestione;
    - vengono registrate su base sistematica le date di ingresso ed uscita dei singoli utenti nei sistemi di uso collettivo come richiesto dalle norme di legge.
5. Il diritto alla riservatezza dell'utente è tutelato dalla deontologia professionale degli amministratori di rete e di sistema, e dalle vigenti normative sulla privacy. Le informazioni in questione devono essere rese disponibili a seguito di formale richiesta dell'Autorita' Giudiziaria (cfr. art. 12).

Art. 11 - CONSEGUENZE DI UN ABUSO

L’utente di risorse informatiche dell’Ateneo che abbia violato di proposito o per incuria il presente Regolamento o la normativa ivi richiamata, sarà

soggetto ad azione disciplinare in conformità a quanto stabilito dai Regolamenti dell'Università, fatta salva la possibilità per l'Ateneo di esercitare le opportune azioni giudiziarie nelle sedi competenti, a tutela dei propri interessi istituzionali.

Art. 12 - ASPETTI LEGALI

A seguito di indagini giudiziarie o azioni legali, l'Ateneo può essere obbligato, dietro formale richiesta delle competenti Autorità, a fornire tracciati relativi all'uso di risorse informative o a consentire l'ispezione di files, floppy disk, nastri, cd-rom, dvd ed altri dispositivi di archiviazione dell'utente localizzati su apparati posseduti ed utilizzati dall'Università.