Norme di attuazione del regolamento dei servizi di rete di Ateneo: accesso ai servizi

Norme utenti

INDICE

PREFAZIONE

Il documento ha lo scopo di evidenziare, dal punto di vista dell'utente finale, le modalità operative consentite, non consentite o illecite, per fruire dei servizi disponibili all'interno della rete dell'Università degli Studi di Modena e Reggio Emilia. La forma del documento è secondo lo stile delle "*domande più frequenti*" per facilitarne la consultazione pratica.

I requisiti tecnologici necessari per poter fruire del servizio richiesto sono descritti nel documento "**Norme di attuazione del regolamento dei servizi di rete di Ateneo: gestione della rete**" e saranno garantiti dalla Direzione Sistemi Informativi e Tecnologie (DSIT) in collaborazione con i **Referenti Informatici per Struttura** che provvederanno ad apportare gli aggiornamenti tecnologici necessari sulla postazione dell'utente.

L'armonizzazione dei comportamenti tramite le norme contenute nel presente documento porta alla riduzione sia dei "rischi" informatici che delle anomalie gestionali, il cui verificarsi influenza in maniera negativa il normale e quotidiano svolgimento delle attività accademiche e amministrative.

La definizione delle norme oggetto del presente documento, dovendo garantire una razionalizzazione delle normali attività lavorative, sarà opportunamente e tempestivamente modificata a fronte di cambiamenti organizzativi o aggiornamenti tecnologici.

A. Norme utente per l'attivazione di attrezzature in rete

1) Chi può utilizzare la rete di ateneo?

Tutti gli utenti, come stabilito dall'art.4 del "Regolamento dei servizi di rete dell'ateneo", possono utilizzare la rete di ateneo.
In particolare gli utenti strutturati e non strutturati hanno diritto di accedere alla rete dal proprio ufficio, oppure dalla propria sede di lavoro abituale (anche con collegamento remoto), oppure tramite computer portatile da ogni posizione universitaria alla quale da cui abbiano necessità di collegarsi.
Gli utenti studenti possono accedere alla rete d'ateneo solo dalle aule informatiche dotate di postazioni fisse appositamente predisposte oppure tramite il loro computer portatile personale solo dalle sedi adeguatamente predisposte[1].

2) Come richiedere l'accesso alla rete di ateneo?

L'utente deve chiedere l'autorizzazione all'accesso alla rete al referente informatico[2] della struttura nella quale vuole usufruire dell'accesso.

1 L'elenco delle sedi che offrono il servizio è accessibile sul sito http://www.dsit.unimo.it

2 L'elenco dei referenti informatici di struttura è mantenuto aggiornato sul sito http://www.dsit.unimo.it

Nel caso di un computer portatile che deve accedere da diverse strutture, la richiesta va effettuata in ciascuna struttura ai rispettivi referenti.

3) Cosa viene richiesto all'utente che si vuole collegare alla rete?

Per tutti l'utilizzo della rete comporta l'assunzione di responsabilità per il proprio comportamento in rete, sia esso attivo che omissivo.
Il richiedente deve indicare nella richiesta il proprio nome quale responsabile dell'attività che svolgerà in rete[3] e le ulteriori informazioni necessarie per l'identificazione dell'attrezzatura da collegare[4].

4) Quali requisiti minimi deve avere l'attrezzatura che si vuole collegare alla rete?

Se è un PC o una Workstations Unix o una stampante che fornisce servizi aggiuntivi[5] deve avere un sistema operativo aggiornabile e aggiornato: sono ammessi i sistemi Windows, Linux, MacOSX, Unix. Per ogni altra apparecchiatura occorre chiedere alla DSIT la valutazione dell'impatto sull'organizzazione e sulla sicurezza della rete.
In particolare l'utente può attaccare alla rete di ateneo access-point o utilizzare software che attiva su una stazione di lavoro le funzionalità di access-point **solamente** richiedendo un **apposito intervento alla DSIT** la quale curerà la realizzazione del collegamento. E' altresì vietato collegare modem alle stazioni di lavoro.

5) Quali protocolli sono ammessi sulla rete di ateneo?

Sulla rete di ateneo sono ammessi i protocolli della famiglia TCP/IP. Chiunque volesse utilizzare protocolli diversi deve riferirlo al referente di struttura e chiedere alla DSIT la valutazione dell'impatto sull'organizzazione e sulla sicurezza della rete.
In particolare vanno disattivati, su tutti i PC con sistema operativo Windows, i protocolli NetBEUI e IPX. Va altresì disattivato sulle stampanti il protocollo IPX.

6) Dopo aver fatto la richiesta che cosa succede?

All'attrezzatura da collegare in rete vengono assegnati i parametri di configurazione IP (indirizzo, netmask, gateway, dns primario e secondario, eventualmente wins) e, associati ad essi, il codice relativo ad una presa di rete a muro[6]. La DSIT si riserva la facoltà di assegnare i parametri di configurazione IP in modalità manuale o automatica.

---

3 Nel caso il richiedente non sia utente strutturato, occorre che la richiesta provenga da uno strutturato ed in questo caso entrambi diventano responsabili.

4 L'elenco aggiornato delle informazioni da fornire è mantenuto sul sito http://www.dsit.unimo.it

5 Gestione via web, server ftp, o altro

6 Nel caso di portatili la presa a muro prevalente.

E' responsabilità dell'utente conoscere tali parametri, che deve mantenere invariati. Pertanto è vietato cambiare autonomamente le impostazioni assegnate all'attrezzatura riguardo ai parametri assegnati o spostare l'attrezzatura in una localizzazione diversa.
Chi avesse necessità di effettuare tali variazioni deve rivolgersi al referente di struttura, il quale ha l'obbligo di mantenere aggiornato il database centralizzato delle informazioni relative alle attrezzature in rete di sua competenza.

7) Quali responsabilità si assume l'utente che lavora in rete?

Essendo la rete di ateneo parte della rete GARR[7], l'utente accetta automaticamente le regole adottate da essa, con particolare riferimento alla "GARR Acceptable Use Policy (AUP)"[8], e le sanzioni da essa previste in caso di trasgressione. Inoltre l'utente è invitato a conoscere e ad attenersi alle regole di "netiquette" previste dagli organismi italiani ed internazionali[9]. Infine l'utente è soggetto alla legislazione vigente dell'ordinamento italiano[10].

8) Cosa fare in caso di cessazione dell'uso dell'indirizzo IP assegnato?

Se un indirizzo per qualsiasi motivo non viene più usato esso deve essere restituito alla DSIT tramite il referente di struttura. Se un'apparecchiatura connessa in rete viene dimessa il suo indirizzo IP deve essere restituito alla DSIT tramite il referente di struttura. L'IP può essere assegnato ad una nuova attrezzatura solo previo accordo con il referente di struttura e comunicazione alla DSIT.

9) Come richiedere l'accesso via modem (RAS)?

L'accesso via modem è riservato agli utenti strutturati, come strumento di lavoro da casa. L'attivazione non è automatica, ma va richiesta tramite il referente di struttura alla DSIT. Nel caso in cui l'accesso sia richiesto per un utente "non strutturato" la domanda va avanzata dal Responsabile del gruppo di lavoro o di ricerca ed occorre indicare il periodo per cui si richiede. L'utente è responsabile delle credenziali di identificazione (username, password, …) assegnate che non possono essere passate ad altri utenti.

10) Come richiedere il collegamento ad enti esterni?

Il collegamento ad enti esterni avviene normalmente attraverso l'uscita Internet verso GARR. Eccezionalmente, in casi particolari, normalmente per

7 http://www.garr.it

8 http://www.garr.it/docs/garr-aup-00.shtml

9 http://www.nic.it/NA/netiquette.txt, RFC 1855 (ftp://ftp.nic.it/rfc/rfc1855.txt), RFC 2635 (ftp://ftp.nic.it/rfc/rfc2635.txt)

10 Si fa riferimento in particolare ai crimini informatici definiti nel Codice penale, al testo unico sulla privacy, al testo unico sul documento elettronico.

motivi di ricerca, può rendersi necessario realizzare collegamenti diretti con enti esterni. In tal caso l'interessato, coinvolgendo anche il referente informatico di struttura, deve richiedere un indagine tecnica alla DSIT per individuare le modalità con la quale realizzare il collegamento e gli eventuali rischi di sicurezza connessi. Tale analisi deve essere allegata alla richiesta da avanzare al CdA per la sua approvazione.
Dopo approvazione da parte del CdA occorre completare la richiesta con una lettera di assunzione di responsabilità da parte del Responsabile richiedente alla DSIT.
E' vietato collegare al proprio computer universitario modem che permettano l'accesso diretto ad enti o provider esterni all'università, senza autorizzazione della DSIT.

B. Obblighi di sicurezza nell'accesso alla rete

11) Come gestire le credenziali di identificazione?

L'università consegna agli utenti delle credenziali di identificazione (username-password, smart-card, certificati, …) per l'accesso a vari servizi.
Le credenziali consegnate sono sempre ad uso personale e non è permesso concederle ad altri, nemmeno ai collaboratori più fidati.
Chi ha necessita di accedere a determinati servizi e non dispone delle credenziali personali, non deve chiederle al collega, ma richiederne il rilascio al gestore del servizio a cui si deve poter accedere.
La componente password della credenziale di identificazione, per qualsiasi servizio si tratti, deve essere non banale, lunga almeno 8 caratteri e modificata almeno ogni 6 mesi.

12) Qual è la protezione globale offerta dall'Ateneo?

La DSIT per mezzo dei suoi sistemi centralizzati (firewall, IDS, antivirus, antispam) mette in opera il massimo che le è possibile a livello di difesa perimetrale. Tuttavia la difesa perimetrale non deve essere considerata alternativa alla difesa personale. E' necessario che ogni utilizzatore sia consapevole che la sicurezza dei proprio computer dipende dalla conoscenza dello stesso e dal compromesso che ciascuno vuole accettare per poter lavorare in rete.

13) Cosa fare per la protezione personale del PC?

Data l'eterogeneità relativa all'utilizzo dei computer in ambiente universitario risulta impossibile decidere una politica globale che garantisca la sicurezza a tutti. Pertanto occorre in tutti la consapevolezza che la sicurezza del proprio PC e di quello degli altri dipende da quanto ciascuno conosce e implementa la sicurezza necessaria per sé sul proprio PC. Ogni PC non sicuro è un pericolo anche per la sicurezza del PC del collega.
L'utilizzatore finale deve:

- Applicare almeno settimanalmente sul proprio PC gli aggiornamenti di sicurezza che vengono periodicamente rilasciati per la propria versione di sistema operativo.
- Mantenere installato l'antivirus sul proprio computer
- Aggiornare l'antivirus almeno settimanalmente (con modalità automatiche o manuali a seconda delle proprie necessità e delle indicazioni della DSIT)
- Effettuare almeno settimanalmente la scansione completa di tutti i dischi del pc per la ricerca e rimozione di eventuali virus
- Utilizzare settimanalmente un programma antispyware seguendo i suggerimenti della DSIT riportati all'indirizzo web http:// _____per scansionare e rimuovere eventuali spyware dal proprio PC
- Installare sul proprio PC un personal firewall seguendo i suggerimenti della DSIT riportati all'indirizzo web http:// _____
- Configurare il personal firewall per permettere il transito in ingresso del solo protocollo ICMP ed eventualmente dei protocolli che ciascuno, dopo attenta valutazione, giudicherà necessari.
- Permettere il traffico in ingresso/uscita al/dal proprio computer solo alle applicazioni conosciute che si ritengono utili per il proprio lavoro e bloccare tutte le rimanenti.
- Attivare la password di BIOS, la password di accesso e la password dello screen saver, al fine di evitare che altre persone possano accedere al computer e carpirne i dati durante la vostra assenza.
- Modificare periodicamente (almeno ogni 6 mesi) le password ed evitare di affidare a Windows la memorizzazione automatica delle stesse (posta elettronica, accesso remoto, etc.). Tutte le password gestite direttamente dal sistema operativo Windows sono altamente insicure. E' consigliabile digitare la password ogni volta che questi servizi vengono utilizzati
- Eseguire periodicamente la pulizia del disco da cookies, file temporanei, etc. e, successivamente, cancellare gli stessi definitivamente con programmi specifici.
- Ricorrere possibilmente alle versioni più recenti del sistema operativo e dei programmi maggiormente utilizzati, con particolare riferimento agli applicativi che consentono l'accesso ad internet.
- Fare spesso il backup dei propri dati su supporto esterno.

14) Cosa fare se il proprio PC ha preso un virus o il proprio PC/server è stato vittima di un intrusione?

1. Staccare il PC compromesso dalla rete
2. Segnalare sempre l'accaduto al proprio referente informatico di struttura, il quale deve segnalare il fatto alla DSIT.
3. Collaborare con il referente e con la DSIT nella compilazione dell'apposito modulo telematico di resoconto sul fatto avvenuto. Sarà cura della DSIT la predisposizione del modulo in linea.

4. Valutare, in caso di grave danneggiamento o di compromissione di dati personali e/o sensibili, se sia il caso di denunciare l'avvenuto alle competenti autorità.
5. Ripristinare il computer seguendo le indicazione della DSIT e del referente informatico di struttura.
6. Ricollegare il computer alla rete solamente dopo essersi assicurati che virus o altro codice maligno sono presenti sul computer.

15) E' possibile l'accesso a dati personali da parte della DSIT?

LA DSIT può accedere ai dati personali senza il consenso dell'Utente qualora si presenti una delle seguenti circostanze:

- nel caso in cui sia necessario identificare o diagnosticare problemi o vulnerabilità presenti nel sistema al fine di preservarne l'integrità;
- su richiesta delle autorità giudiziarie;
- 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.

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. La DSIT ha in ogni caso la facoltà di conservare traccia dell'attività relativa all'uso dei servizi di rete senza alcun consenso.

16) L'utente viene monitorato quando lavora in rete?

All'atto della connessione di un elaboratore alla Rete d'Ateneo, l'Utente autorizza automaticamente la DSIT ad utilizzare sistemi in grado di verificarne il livello di sicurezza e a mantenere i files di log, cioè archivi contenenti elenchi descrittivi relativi alle risorse di rete utilizzate dai singoli Utenti.

C. Norme per l'accesso ai servizi di rete centralizzati

17) Quali sono i servizi di rete offerti agli utenti?

Servizi per i quali sono richieste credenziali di identificazione:

- Servizio di posta elettronica @unimore.it (mailbox, alias, iscrizione alle liste di distribuzione)
- Ospitalità siti web
- Spazio web personale
- Forum di discussione
- Accesso ai servizi amministrativi quali ESSE3, CSA, CIA, Gestime, Titulus, Tools di accesso alle banche dati

Le modalità di rilascio delle credenziali per ognuno di questi servizi sono indicate sul sito della DSIT.

Servizi per i quali non sono richieste credenziali di autenticazione:

- navigazione Internet
- ftp anonimo

18) Norme generali valide per tutti i servizi ad accesso personalizzato

L'accesso ai servizi in rete è consentito solo a chi, avendone fatto esplicita richiesta personale, ne abbia ottenuto l'autorizzazione. Unica eccezione è il servizio di posta elettronica che viene fornito automaticamente a tutti gli utenti al momento della presa di servizio o dell'iscrizione se studenti.
L'autorizzazione è data con la consegna delle credenziali personali di identificazione. Le credenziali vanno conservate privatamente e non cedute a terzi.

19) Norme valide per i servizi non protetti

I servizi di informazione, quali il web, o altri servizi di ausilio, quali il servizio di ftp anonimo, non richiedono credenziali di identificazione per potervi accedere. Tuttavia l'uso di questi servizi è consentito nei limiti dei percorsi predisposti e comunque non in violazione di legge.

20) Norme e consigli da osservare nell'uso della Posta Elettronica

- La mailbox non può essere utilizzata per propaganda politica o elettorale esterna all'Ateneo
- Non si possono inviare messaggi allo scopo di molestare o minacciare
- Occorre ricordare che l'uso della posta elettronica è consentito nelle norme previste dal Codice Civile e Penale, sono violazioni la divulgazione tramite posta elettronica di materiale osceno, la ricezione, trasmissione o possesso d'immagini pornografiche relative a minori
- Non rispondere ai messaggi di posta "non sollecitati", chiedendo di essere cancellati da quella lista di invio: in tal modo rischiate di fare il gioco di chi li ha spediti, facendogli capire che la vostra casella di posta è attiva.
- Non comunicare la propria mail a siti ai quali non si è veramente interessati e/o sui quali avete anche il minimo dubbio.
- Evitare di girare i falsi allarmi e le catene di S. Antonio, rivolgendosi alla DSIT per controllare preventivamente la bontà delle informazioni
- Non aprire messaggi di posta elettronica e eseguire files allegati ai messaggi senza preventiva scansione antivirus
- Non dare credito a un messaggio pubblicitario dalle caratteristiche sospette (spesso di natura erotica o che promette facili guadagni) che reindirizza ad un sito internet "per saperne di più";
- Evitare di inviare posta elettronica in formato "html" che, seppure consente una forma più elegante e/o simpatica, è uno dei metodi più subdoli per veicolare contenuti virus, worm e frodi (senza necessità di allegati).

21) Consigli da osservare nella navigazione in Internet

- L'utilizzo di Internet è consentito nelle norme previste dal Codice Civile e Penale, sono violazioni la divulgazione tramite internet di materiale osceno, la ricezione, trasmissione o possesso d'immagini pornografiche relative a minori, la violazione di coyright
- Non navigare su siti di Hacking, cracking, ecc, senza apposite protezioni;
- Non scaricare software da siti poco attendibili o non ufficiali;
- Non installare programmi scaricati da siti non ufficiali o comunque di natura incerta;
- Tenere sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti sulla vostra macchina. Disattivate sul browser l'esecuzione automatica degli script Java e ActiveX;
- Mentre si naviga prima di selezionare un link, posizionarsi sopra il cursore del mouse e osservarne il percorso sulla apposita barra del browser: se è un file eseguibile non seguire mail il link.

D. Norme per l'attivazione di servizi pubblici e privati

SERVIZIO PUBBLICO: è un servizio informatico rivolto alla totalità degli utenti e/o al WEB, accessibile senza password o identificazione personale.

SERVIZIO PRIVATO: è un servizio informatico rivolto esclusivamente ad una specifica categoria di persone o enti (ricercatori, studenti, aziende, enti pubblici, ecc.) allo scopo di facilitare una collaborazione scientifica, didattica o amministrativa. Questo servizio di norma è abilitato attraverso la richiesta di credenziali d'identificazione personale (password, smart card, ecc.)

22) E' possibile attivare servizi al pubblico diversi da quelli offerti dalla DSIT?

L'apertura di servizi al pubblico, quali servizi web, servizi multimediali, servizi di condivisione files, server SMTP autonomo, è condizionata alle verifiche di sicurezza che devono essere fatte dalla DSIT. Inoltre ogni servizio al pubblico deve avere il proprio responsabile tecnico oltre che il responsabile dei contenuti. Si rimanda al sito della DSIT per le modalità di richiesta.

23) E' possibile attivare servizi privati verso collaboratori scientifici esterni all'università?

L'apertura di servizi privati verso collaboratori scientifici esterni deve essere richiesta alla DSIT dal responsabile del servizio. L'accesso da parte di esterni deve sempre avvenire tramite credenziali di validazione dell'identità personali e non cedibili

24) E' possibile dare la gestione remota delle apparecchiature alle ditte venditrici o a consulenti a scopo di manutenzione?

L'accesso alle apparecchiature universitarie anche a scopo di manutenzione deve essere concordato con la DSIT in modo da garantire le necessarie precauzioni di sicurezza. E' necessario fornire alla DSIT i riferimenti della ditta/persona che accederà alle apparecchiature. La ditta/persona dovrà essere messa a conoscenza delle Norme gestionali e delle Nome utente. L'accesso da esterno richiede sempre la validazione dell'identità tramite credenziali personali non cedibili.

E. Procedure da seguire in caso di malfunzionamenti

25) Non funziona la rete o uno/più servizi di rete: che cosa devo fare?

Il mancato funzionamento può derivare da un guasto della rete o sei servizi, oppure perché l'apparecchiatura è stata bloccata dalla DSIT a seguito della rilevazione di un problema hardware e/o software dell'apparecchiatura stessa, ovvero in seguito ad uso improprio.
Occorre rivolgersi al referente informatico di struttura che si coordinerà con la DSIT per i necessari controlli e l'eventuale ripristino.

26) Quali sono i motivi per cui posso avere la presa rete o l'IP bloccato?

MOTIVAZIONI TECNICHE

La DSIT ha la facoltà di bloccare l'indirizzo IP o disattivare la presa di rete se vengono riscontrate violazioni rispetto agli articoli contenuti in queste norme, o nel caso che compromettano la normale fruizione dei servizi.
La DSIT ha la facoltà di impedire l'accesso in rete a tutte le apparecchiature che risultino affette da virus, generino spam o diffondano/eseguano codice maligno, o semplicemente facciano traffico sproporzionato. La DSIT ha anche la facoltà di bloccare l'accesso in rete ad intere strutture se da esse proviene un traffico di rete dannoso al funzionamento della rete nel resto dell'ateneo.
La DSIT 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.

MOTIVAZIONI GENERALI DI ACCESSO AI SERVIZI DI RETE

Le modalità di accesso ai servizi sono regolate mediante l'assegnazione di user-id e password di accesso personali e segrete; devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le password non devono contenere riferimenti agevolmente riconducibili all'utente (es. nomi dei familiari, ecc.).

L'accesso ai servizi di rete, sia Internet che Intranet, è regolato dalle norme emanate dalla Commissione per l'Informatica e la Rete di Ateneo (CIRA) e gestite dalla DSIT ed è consentito esclusivamente per fini istituzionali, ovvero

per attività che non arrechino danno ad altri utenti o all'Ateneo stesso e siano conformi al documento "Regolamento dei servizi di rete di Ateneo". Tra queste attività non consentite, e definite proibite o illecite, si fa specifico riferimento a:

- violazione della privacy di altri utenti;
- violazione dell'integrità di dati personali;
- compromissione dell'integrità dei sistemi o dei servizi;
- consumo di risorse o utilizzo dei servizi di rete in misura tale da impedire / compromettere l'efficienza di altri servizi di rete o in modo tale da causare danno alle attività di altri utenti;
- utilizzo incompatibile con lo status "no-profit" dell'Ateneo e/o violazione di contratti Universitari;
- compimento di atti di criminalità informatica compreso il danneggiamento dei Sistemi in Rete dell'Ateneo o di altre organizzazioni o il tentativo di violazione dei loro sistemi;
- distribuzione di virus informatici, modifica o rimozione di dati o apparati di rete aumentando così la vulnerabilità del sistema;
- utilizzo degli strumenti per fini terroristici, pornografici, pedofili o comunque per attività ritenute illegali dalla legislazione vigente.

Possono verificarsi circostanze nelle quali l'amministratore del sistema (la DSIT), secondo quanto stabilito dalla legge, ha il diritto di accedere ai dati personali anche in assenza del consenso dell'Utente. Più precisamente:

- nel caso in cui sia necessario, previa esplicita richiesta da parte degli Organi Accademici o delle Autorità Giudiziarie, identificare o diagnosticare problemi di vulnerabilità presenti nel sistema al fine di preservarne l'integrità;
- 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.

In accordo con il diritto alla privacy dell'Utente, l'accesso ai dati personali può in ogni caso avvenire previo consenso del Rettore. La DSIT ha in ogni caso il diritto / necessità di conservare traccia dell'attività degli Utenti relativa all'utilizzo dei servizi di rete senza alcun consenso; tali informazioni saranno utilizzate esclusivamente a fronte di esplicite richieste del Rettore o delle Autorità Giudiziarie.

Al fine del periodo di utilizzazione del sistema, o anche in caso di inutilizzo dello stesso per lungo tempo (pausa pranzo o altro) l'utente è tenuto ad effettuare l'operazione di log-out, ovvero a scollegarsi dal sistema stesso onde evitare possibili utilizzi fraudolenti del supporto informatico collegato con i propri codici di accesso.

MOTIVAZIONI SPECIFICHE CONNESSE AI SERVIZI INTERNET

Per quanto riguarda la fruizione di servizi attraverso la rete internet da postazioni dell'Ateneo si evidenzia in particolare che:

- l'utilizzo di internet è consentito nelle norme previste dal Codice Civile o Penale. Sono esempi di palese violazione la divulgazione tramite internet di schemi piramidali, la distribuzione di materiale osceno, la ricezione, trasmissione o possesso d'immagini pornografiche relative a minori, violazione di copyright, utilizzo dello strumento per fini terroristici. Specifiche deroghe alle limitazioni su citate saranno valutate e concesse, da parte degli Organi competenti, a fronte di documentate motivazioni scientifiche e/o professionali.
- ogni struttura universitaria che inserisca documenti su web (accessibili sia dall'interno, INTRANET, che dall'esterno INTERNET), è responsabile dei contenuti pubblicati.

F. Procedure da seguire per l'attivazione di servizi amministrativi

27) Quali sono i servizi amministrativi che posso attivare?

Servizio	Richiedente / Autorizzazione	Modalità di richiesta
Servizi di accesso al data base (ORACLE o altri) nel caso siano estesi al di fuori della propria sottorete;	• Responsabile della struttura a cui appartiene lo "strutturato" che deve fruire del servizio. • Responsabile del gruppo di lavoro o di ricerca nel caso in cui il servizio sia richiesto per una risorsa "non strutturata".	Mail di richiesta alla DSIT, alla attenzione del Responsabile dei Servizi Gestionali
Attivazione programma contabilità generale ed economica (CIA)	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso CIA al Direttore della Area Economico Finanziaria • Dopo autorizzazione accesso CIA; mail di richiesta attivazione utente / password alla DSIT (att.ne R. Messori)
Attivazione programma gestione risorse umane (CSA)	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso CSA al Dirigente della Area Risorse Umane • Dopo autorizzazione accesso CSA; mail di richiesta attivazione utente / password alla DSIT (att.ne R. Messori)
Attivazione programma gestione segreterie studenti (ESSE3)	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso ESSE3 al Dirigente della Area Didattica e Ricerca • Dopo autorizzazione accesso ESSE3; mail di richiesta attivazione utente / password alla DSIT (att.ne M. Orlandi)
Attivazione programma gestione delle timbrature di entrata / uscita (GESTIME)	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso GESTTIME al Dirigente della Area Risorse Umane • Dopo autorizzazione accesso GESTTIME; mail di

		richiesta attivazione utente / password alla DSIT (att.ne R. Turrini)
Attivazione programma gestione protocollo (TITULUS)	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso TITULUS al Dirigente della Area Affari Generali • Dopo autorizzazione accesso TITULUS; mail di richiesta attivazione utente / password alla DSIT (att.ne A. Ghidoni)
Attivazione programma "Gestione Riferimenti"	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso al programma "Gestione Riferimenti" alla DSIT (att.ne D. Ferrari / M. Orlandi)
Attivazione accessi alle biblioteche on-line	Richiesta di attivazione di utente / password emessa dal Responsabile della struttura all'interno della quale opera la risorsa che deve usare il programma	• Mail di richiesta autorizzazione accesso al programma al Presidente del CSBA • Dopo autorizzazione accesso da parte di CSBA; mail di richiesta attivazione utente / password alla DSIT (att.ne D. Maccari / L. Magnani)