



REGOLAMENTO UTILIZZO INTERNET E POSTA ELETTRONICA

Premesse

Il Regolamento è un atto dovuto e previsto dal provvedimento del Garante per la Privacy pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007. Tale provvedimento, in seguito a diverse segnalazioni e quesiti posti al garante in merito al trattamento di dati personali con strumenti informatici, prescrive ai datori di lavoro pubblici e privati di stilare un disciplinare relativo all'utilizzo di internet e della posta elettronica nei posti di lavoro indicando in che misura e con quali modalità siano effettuati eventuali controlli.

Nelle indicazioni che il garante suggerisce sono previsti anche interventi sulle apparecchiature di rete per garantire il rispetto del Regolamento (per es. limitare l'accesso a particolari siti). Non ritenendo facilmente attuabili tali interventi, anche per la specificità dell'attività di un Ateneo, si è ritenuto opportuno stilare semplicemente delle norme di comportamento. Si potrebbero mettere in atto eventualmente controlli di tipo generico sul rispetto di tali norme da effettuare in maniera anonima.

Il Regolamento è stato stilato facendo riferimento alla policy di utilizzo della rete da parte del Garr, la rete della ricerca che consente la connettività dell'Ateneo verso Internet

DISCIPLINARE IN MERITO ALL'UTILIZZO DELLA POSTA ELETTRONICA E DI INTERNET

Art. 1 – Caratteri generali

Il presente Regolamento, nel rispetto del regolamento sul trattamento dei dati personali, sensibili e giudiziari, disciplina le modalità di utilizzo delle risorse informatiche dell'Ateneo, l'accesso e l'utilizzo della rete di Ateneo e dei servizi che, tramite la rete, è possibile ricevere e offrire all'interno ed all'esterno della rete dell'Università Politecnica delle Marche.

La rete telematica dell'Università Politecnica delle Marche fa parte dell'infrastruttura di rete telematica nazionale denominata "GARR – La Rete Italiana dell'Università e della Ricerca Scientifica", di cui utilizza i servizi di collegamento e di interoperabilità che permettono di accedere alla rete internet. L'uso della rete di Ateneo è pertanto subordinato al rispetto da parte di tutti gli utenti oltre che del presente Regolamento anche delle norme dettate dagli organi di governo del GARR.

Le norme relative all'uso della rete GARR fanno parte integrante del presente Regolamento (Allegato A).

Art. 2 – Sviluppo e gestione

La rete interna di Ateneo collega tutte le strutture dell'Università e, tramite la rete GARR, fornisce i servizi di posta elettronica e l'accesso alla rete Internet a tutte le stazioni di lavoro informatiche attestata sulla rete stessa. Lo sviluppo e la gestione della rete è affidata al

Centro Servizi Multimediali e Informatici che opera conformemente alle delibere degli organi accademici ed in stretta collaborazione con il GARR stesso.

Art. 3. – Gestione indirizzamento IP e domini

La gestione e il monitoraggio della rete TCP/IP dell'Università e la gestione del dominio univpm.it e dei relativi sottodomini sono di competenza esclusiva del CESMI.

Il CeSMI, in quanto responsabile amministrativo e tecnico dello spazio di indirizzamento IP e del dominio univpm.it assegnato all'Ateneo dalle autorità competenti nazionali e internazionali deve garantire costantemente il rispetto di tutte le leggi e le normative vigenti.

La richiesta di uno o più indirizzi IP da parte di un utente deve avvenire tramite un'apposita domanda al CeSMI, a firma dell'utente stesso e del Responsabile della struttura di appartenenza, nella quale risulti l'accettazione del presente Regolamento. Nel momento in cui un indirizzo IP non venga più utilizzato dall'utente richiedente dovrà esserne data immediata comunicazione scritta da parte del Responsabile della struttura.

La richiesta di una sottorete o di un insieme di indirizzi IP da parte di una struttura dell'ateneo deve avvenire tramite un'apposita domanda al CeSMI, a firma del Responsabile della struttura, nella quale risulti il nome dell'eventuale Referente Informatico delegato e l'accettazione del presente Regolamento. In questo caso è compito e obbligo del Responsabile della struttura o del Referente Informatico delegato assegnare gli indirizzi IP all'interno della struttura provvedendo sempre a mantenere aggiornata, con uno storico di almeno due anni, la lista delle coppie "**Indirizzo IP – Nome Utente**" assegnate. Nel caso di assegnazioni dinamiche (DHCP) degli indirizzi IP è compito e obbligo del Responsabile della struttura o del Referente Informatico delegato mantenere, con uno storico di almeno due anni, la lista delle coppie "**Indirizzo IP – Nome Utente**" assegnate dinamicamente dal sistema.

La richiesta di un sottodominio del dominio univpm.it (es: xxx.univpm.it) da parte di una struttura dell'ateneo o di un suo utente deve avvenire tramite un'apposita domanda al CeSMI, a firma del Responsabile della struttura ed eventualmente dell'utente richiedente, nella quale risulti il nome del Responsabile del sottodominio e l'accettazione del presente Regolamento.

Non è consentito collegare alla rete di Ateneo, anche tramite collegamento WiFi, attrezzature di calcolo personali o comunque non di proprietà dell'Università Politecnica delle Marche (desktop, notebook, palmari, smartphone) se non preventivamente autorizzate dal Responsabile della struttura dove l'attrezzatura va collegata o direttamente dal CESMI. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente Regolamento.

Non è inoltre consentito collegare alla rete di Ateneo apparati di rete (Access Point WiFi, router, switch, ...) se non preventivamente autorizzati dal CESMI. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente Regolamento.

Art 4. – Utenti rete Ateneo



Sono collegate alla rete di Ateneo tutte le strutture didattiche, di ricerca e di servizio dell'Università Politecnica delle Marche.

Possono richiedere il collegamento Enti esterni all'Università Politecnica delle Marche in seguito a convenzioni, approvate dagli organi accademici, comprovanti la collaborazione e la necessità della connessione. La struttura esterna deve comunque nominare un referente per il collegamento e comunicarlo al CESMI.

Tutti gli utenti che a qualsiasi titolo utilizzano la rete di Ateneo accettano senza riserve il presente Regolamento.

Art. 5 - Autorizzazioni

Ciascun utente accede alla rete di Ateneo ed alle sue risorse utilizzando delle credenziali costituite da un nome utente ed una password.

Per il personale docente, il personale tecnico amministrativo, gli studenti, i dottorandi, gli specializzandi il nome utente e la password sono assegnati automaticamente dalle procedure informatiche amministrative, per tutti gli altri utenti non strutturati le credenziali sono assegnate dal CESMI previa richiesta opportunamente autorizzata. I criteri di assegnazione delle credenziali sono disponibili nell'allegato B.

Art. 6 – Credenziali di accesso

Le credenziali di accesso (nome utente e password) sono strettamente personali ed ogni attività non regolare sarà imputata al titolare delle credenziali.

Gli utenti sono tenuti a conservare le proprie credenziali mantenendo segrete le modalità di accesso avendo cura che non siano utilizzate da terzi. Gli utenti dovranno prontamente avvisare il CESMI in caso di smarrimento o anche di probabile diffusione dei dati di accesso alla rete.

Art. 7 – Utilizzo computer, periferiche, materiale di consumo

Sui computer di proprietà dell'Università Politecnica delle Marche non è consentito:

- Installare programmi non inerenti l'attività lavorativa e/o privi di licenze d'uso legali
- Installare antivirus, antispyware e firewall non autorizzati
- Modificare le configurazioni relative all'accesso alla rete di ateneo comunicate al momento della installazione (es. numero IP)
- Attivare l'accesso dall'esterno ad un sistema di calcolo se non preventivamente comunicato al CeSMI o al Responsabile della struttura.
- Installare modem per l'accesso da/all'esterno se non preventivamente autorizzati
- Connettere dispositivi esterni personali (chiavi usb, hard disk, ecc.) se non preventivamente autorizzati



- Copiare su dispositivi esterni personali dati la cui titolarità è dell'Università Politecnica delle Marche

L'utilizzo delle stampanti e dei materiali di consumo (carta, toner, CD-Rom, DVD, chiavi USB) è riservato alla preparazione di materiale didattico, scientifico, amministrativo o comunque inerente l'attività istituzionale dell'Ateneo

Art. 8 – Rete internet

L'utilizzo di internet è consentito:

- a tutto il personale, a tempo determinato ed indeterminato, dell'Università Politecnica delle Marche per lo svolgimento delle proprie attività istituzionali inerenti la ricerca, la didattica, le funzioni amministrative mediante le attrezzature informatiche messe loro a disposizione
- a tutto il personale titolare di borsa di studio, di assegno di ricerca, di contratto per lo svolgimento delle proprie attività
- agli studenti regolarmente iscritti ai corsi di laurea, ai dottorati di ricerca, alle scuole di specializzazione dell'ateneo mediante l'utilizzo delle aule attrezzate a loro disposizione o mediante attrezzature proprie autorizzate collegate alla rete WiFi dell'Ateneo

Sulla rete non sono ammesse le seguenti attività:

- navigare e/o registrarsi su siti non inerenti la propria attività istituzionale, didattica e di ricerca
- scaricare programmi e/o file coperti da diritto d'autore se non espressamente autorizzati
- partecipare a forum o chat line se non per motivi relativi alla propria attività istituzionale
- conservare file a contenuto discriminatorio
- tentare accessi fraudolenti a dati, programmi e sistemi altrui
- utilizzare credenziali di accesso diverse da quelle di cui si è assegnatari

Art. 9 – Posta elettronica

L'utilizzo della posta elettronica è consentito:

- a tutto il personale, a tempo determinato e indeterminato, dell'Università Politecnica delle Marche mediante una casella di posta istituzionale, assegnata dall'ateneo stesso, nella forma n.cognome@univpm.it oppure per i casi di omonimia nome.cognome@univpm.it
- a tutti gli studenti iscritti ai corsi di laurea, dottorandi, specializzandi, studenti Erasmus mediante la casella di posta assegnata dall'ateneo (nella forma



Snnnnnnn@studenti.univpm.it dove nnnnnnn è il numero di matricola) o mediante una propria casella di posta che deve essere registrata nei loro dati anagrafici

- ad ogni utente autorizzato a qualsiasi titolo ad accedere alla rete di ateneo dal Responsabile della struttura
- ad ogni struttura dell'Ateneo mediante una casella di posta nella forma *nomestruttura@univpm.it*

Art. 10 – Modalità utilizzo caselle di posta istituzionali e personali

Le modalità di utilizzo della posta elettronica a cui attenersi sono le seguenti:

- non è consentito l'utilizzo delle caselle di posta elettronica dell'ateneo per attività personali non attinenti le proprie mansioni e la propria attività istituzionale
- la casella di posta di ogni singola struttura può essere utilizzata da più dipendenti secondo quanto stabilito dal responsabile della struttura stessa
- in caso di assenza prolungata o improvvisa il singolo dipendente deve essere messo in condizioni di delegare un altro dipendente a leggere i propri messaggi e inoltrare quelli ritenuti importanti per lo svolgimento dell'attività lavorativa
- il personale può comunque, previa autorizzazione ed in via eccezionale, utilizzare una propria casella di posta elettronica non istituzionale. In questo caso, se l'accesso avviene tramite postazioni di lavoro di proprietà dell'Università Politecnica delle Marche, la casella di posta può essere consultata solo in modalità webmail
- le caselle personali non istituzionali non possono essere utilizzate per l'attività istituzionale
- l'uso della posta elettronica non è comunque consentito per partecipare a forum e/o dibattiti se non per motivi istituzionali, per diffondere notizie non veritiere o quanto altro che abbia contenuto offensivo e discriminatorio, per inviare lettere a catena ovvero messaggi ripetuti
- e' fatto divieto di inviare messaggi con contenuti che non rispettino la normativa sulla proprietà intellettuale

Art. 11 – Mailing List

Sono costituite le mailing list di tutto il personale dell'Ateneo suddivise per categoria e per funzioni (Allegato C). L'iscrizione alle mailing list è automatica una volta assegnata la casella di posta istituzionale.

Le mailing list sono adibite alla diffusione d'informazioni di interesse generale e comunque di servizio rivolte al personale.

Hanno diritto ad utilizzare le mailing list del personale:

- Il Rettore
- Il Prorettore



- Il Direttore Amministrativo

Il Rettore può estendere l'utilizzo alle organizzazioni sindacali rappresentate nell'Ateneo e ad altri soggetti interni all'Ateneo compresi i membri degli organi di governo che ne facciano espressa richiesta.

Art. 12 – Comunicazioni mediante posta elettronica

Le comunicazioni via posta elettronica non sostituiscono le comunicazioni formali su supporto cartaceo. Tali comunicazioni possono essere utilizzate per:

- richiedere o concedere ferie e permessi
- convocare riunioni
- inviare comunicazioni di servizio anche dirette al singolo dipendente
- diffondere circolari
- trasmettere copia elettronica di documenti redatti su supporti cartacei (purché in formati e dimensioni opportune)

Art. 13 – Responsabilità individuali

I soggetti che utilizzano risorse informatiche all'interno della rete di Ateneo sono tenuti a:

- mantenere un'adeguata riservatezza dei dati
- mantenere un'adeguata riservatezza sulle misure di sicurezza adottate e sulle modalità di accesso ai servizi
- utilizzare esclusivamente le risorse alla cui fruizione sono autorizzati
- segnalare ogni accertata violazione delle norme del presente Regolamento

Art. 14 – Trattamento dati di accesso

Le attività di accesso ai servizi Internet ed alla posta elettronica sono registrate in forma elettronica. L'attività di registrazione avviene attraverso dei file di sistema a cura del CESMI o dei Responsabili di eventuali sistemi NAT installati localmente che ne garantiscono la custodia e la riservatezza. I file sono mantenuti per un periodo di due anni

I dati personali relativi all'utente, alle sue attività ed ai contenuti che sono immessi in rete non sono sottoposti a trattamenti se non ai fini di legge o in relazione alle richieste dell'autorità giudiziaria.

I dati relativi alle connessioni sono gestiti in maniera anonima e trattati esclusivamente in relazione alle attività di monitoraggio del servizio, alla sicurezza ed all'integrità dei sistemi.

Art. 15 - Violazioni



E' vietata qualsiasi attività che possa produrre danni alle risorse informatiche dell'Università o comunque illecita. A titolo esemplificativo, costituisce infrazione:

- qualsiasi atto che possa compromettere la sicurezza e la riservatezza delle risorse informatiche dell'Università o di altri Enti fruibili attraverso le stesse risorse
- l'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse informatiche anche mediante credenziali di accesso rese disponibili da altre soggetti, nonché l'abbandono senza custodia o senza protezione di stazioni di lavoro già connesse alla rete di Ateneo
- l'uso di dati o di altre risorse informatiche per scopi non consentiti dal presente Regolamento
- l'utilizzo per scopi di interesse esclusivamente privato di qualsiasi risorsa dell'Università
- qualunque altra attività in contrasto con il presente Regolamento

Art. 16 – Sanzioni

La contravvenzione al presente Regolamento comporta la revoca delle autorizzazioni ad accedere alle risorse informatiche gestite dall'Università fatte salve le più gravi sanzioni previste dalle norme vigenti.

Il Responsabile del CESMI, avuta notizia dell'infrazione e valutata la gravità della stessa, provvede ad informare l'organo competente.



Allegato A.

ACCEPTABLE USE POLICY GARR

1. La Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "la Rete GARR", si fonda su progetti di collaborazione scientifica ed accademica tra le Università, le Scuole e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di Rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà, quali quelle afferenti ad altri Ministeri che abbiano una Convenzione specifica con il Consortium GARR, oppure realtà che svolgono attività di ricerca in Italia, specialmente, ma non esclusivamente, in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al MIUR. L'utilizzo della Rete è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.
2. Il "Servizio di Rete GARR", definito brevemente in seguito come "Rete GARR", è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità (operati direttamente o per conto del Consortium GARR) che permettono ai soggetti autorizzati ad accedere alla Rete di comunicare tra di loro (Rete GARR nazionale).
Costituiscono parte integrante della Rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la Rete GARR nazionale e le altre reti.
3. Sulla rete GARR non sono ammesse le seguenti attività:
 - fornire a soggetti non autorizzati all'accesso alla Rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonché permettere il transito di dati e/o informazioni sulla Rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla Rete GARR (third party routing);
 - utilizzare servizi o risorse di Rete, collegare apparecchiature o servizi o software alla Rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete GARR e su quelle ad essa collegate;
 - creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
 - trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
 - danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di



- parole di accesso (password), chiavi crittografiche riservate e ogni altro “dato personale” come definito dalle leggi sulla protezione della privacy;
- svolgere sulla Rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonché dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di Rete cui si fa accesso.
4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la Rete è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la responsabilità può coinvolgere anche le persone che la legge indica come tutori dell'attività dei minori.
 5. I soggetti autorizzati (S.A.) all'accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete per tutte le proprie attività istituzionali. Si intendono come attività istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purchè l'utilizzo sia a fini istituzionali. Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.
Altri soggetti, autorizzati ad un accesso temporaneo alla Rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.
Il giudizio finale sulla ammissibilità di una attività sulla Rete GARR resta prerogativa degli Organismi Direttivi del Consortium GARR.
 6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.
Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR.
 7. È responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.
 8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi del Consortium GARR.



9. In caso di accertata inosservanza di queste norme di utilizzo della Rete, gli Organismi Direttivi del Consortium GARR prenderanno le opportune misure, necessarie al ripristino del corretto funzionamento della Rete, compresa la sospensione temporanea o definitiva dell'accesso alla Rete GARR stessa.
10. L'accesso alla Rete GARR è condizionato all'accettazione integrale delle norme contenute in questo documento.



Allegato B.

Modalità assegnazione credenziali di accesso

Personale docente e tecnico amministrativo.

Codice utente. Al personale docente e tecnico amministrativo le credenziali sono assegnate in automatico dalla procedura di gestione della carriera economica e giuridica del personale (CSA) al momento dell'assunzione. Una volta inseriti i dati anagrafici, al dipendente è assegnato un numero di matricola costituito da 6 cifre. Il codice utente sarà allora costituito dalla lettera P seguita dal numero di matricola (es. per la matricola 1245 il codice utente per l'accesso ai servizi informatici ed alla rete di ateneo sarà P001245).

Password. La password iniziale assegnata ad ogni utente è costituita dal proprio codice utente seguito da giorno e mese di nascita ognuno composto da due cifre (es. per matricola 1245 nata il giorno 24 del mese di febbraio, la password iniziale sarà P0012452402). Al primo accesso nell'area riservata del portale di ateneo sarà richiesto di modificare la propria password in modo che questa sia conosciuta esclusivamente per il singolo utente.

Studenti dei corsi di laurea, dottorandi, specializzandi.

Codice utente. A qualsiasi studente iscritto ai corsi di laurea triennali, corsi di laurea specialistica, dottorando di ricerca, scuola di specializzazione, le credenziali sono assegnate in automatico dalla procedura di gestione della carriera didattica degli studenti (GISS) al momento dell'immatricolazione. Una volta inseriti i dati anagrafici, allo studente è assegnato un numero di matricola costituito da 6 cifre. Il codice utente sarà allora costituito dalla lettera S seguita dal numero di matricola (es. per la matricola 2325 il codice utente per l'accesso ai servizi informatici ed alla rete di ateneo sarà S002325).

Password. La password iniziale assegnata ad ogni utente di questa categoria è costituita dal proprio codice utente seguito da giorno e mese di nascita ognuno composto da due cifre (es. per matricola 2325 nata il giorno 3 del mese di marzo, la password iniziale sarà S0023250303). Al primo accesso nell'area riservata del portale di ateneo sarà richiesto di modificare la propria password in modo che questa sia conosciuta esclusivamente per il singolo utente.

Altre categorie di utenti.

Qualsiasi altra categoria di utenti che non ricada nelle precedenti e che a qualsiasi titolo abbia diritto ad usufruire dell'accesso alla rete di Ateneo ed ai servizi connessi, deve fare espressa richiesta al CESMI per ottenere le credenziali di accesso alla rete. Il CESMI provvederà a consegnare le suddette credenziali in busta chiusa e sigillata. L'utente al primo accesso all'area riservata del portale di Ateneo sarà obbligato a modificare la password a lui assegnata in modo che la stessa sia di sua esclusiva conoscenza.



ALLEGATO C

Mailing List personale

Mailing List a iscrizione automatica

- Personale Tecnico Amministrativo
- Personale Docente
- Direttori Dipartimento
- Direttori Istituto