UNIVERSITÀ DEGLI STUDI DI PALERMO

AREA AFFARI GENERALI E LEGALI
SETTORE AFFARI LEGALI GENERALI E PRIVACY

Titolo I	Classe 6	Fascicolo 1
N. 25842	del 02-04-2012	
UOR SCT. 45	CC	RPA NUARA

DECRETO N. 1249/2012

IL RETTORE

Visti gli artt. 2 e 15 della Costituzione;
Visto l'allegato VII, par. 3 del D. Lgs. 19 settembre 1994 , n. 626 e s.m.i.;
Visto il D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";
Visto il provvedimento dell'Autorità Garante per la Protezione dei dati Personali del 01/03/2007 n. 13 "Linee guida per posta elettronica ed Internet" pubblicato in G.U. n. 58 del 10/03/2007;
Vista la direttiva n. 2 del 26 maggio 2009 del Ministro per la Pubblica Amministrazione e l'Innovazione "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro";
Visto il Regolamento d'Ateneo per il trattamento dei dati personali. Istruzioni organizzative e tecniche;
Visto il Regolamento d'Ateneo per il trattamento dei dati sensibili e giudiziari;
Visti gli artt. 2 e 49 D. Lgs. 7 marzo 2005 n. 82, Codice dell'Amministrazione digitale.

DECRETA

È emanato il Disciplinare sull'utilizzo della rete Internet e della e- mail adottato con deliberazione consiliare il 14 febbraio 2012 per come appresso riportato.

"Disciplinare
sull'utilizzo della rete Internet e della e- mail"

Art. 1
Principi generali

Il presente Disciplinare ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio Internet e del servizio e-mail da parte del personale dell'Università degli Studi di Palermo, denominata d'ora innanzi UNIPA, e di altri Utenti secondo le definizioni di cui all'art. 3 del presente disciplinare.

Il Disciplinare viene emanato nel rispetto delle seguenti disposizioni normative e regolamentari:
- artt. 2 e 15 della Costituzione;
- allegato VII, par. 3 del D. Lgs. 19 settembre 1994 , n. 626 e s.m.i.;

- D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" e provvedimenti successivi del Garante della Privacy;
- provvedimento dell'Autorità Garante per la Protezione dei dati Personali del 01/03/2007 n. 13 "Linee guida per posta elettronica ed Internet" pubblicato in G.U. n. 58 del 10/03/2007;
- direttiva n. 2 del 26 maggio 2009 del Ministro per la Pubblica Amministrazione e l'Innovazione "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro";
- regolamento d'Ateneo per il trattamento dei dati personali. Istruzioni organizzative e tecniche;
- regolamento d'Ateneo per il trattamento dei dati sensibili e giudiziari;
- D. Lgs. 30 Dicembre 2010 n. 325, Codice dell'Amministrazione Digitale (CAD).

L'infrastruttura di rete di UNIPA è articolata sul territorio metropolitano e sui poli didattici di Agrigento, Caltanissetta e Trapani; l'accesso ad Internet avviene attraverso l'infrastruttura di rete per l'Università e la Ricerca gestita dal "*Consortium* GARR – Gruppo Armonizzazione Reti della Ricerca"; il nodo GARR per la Sicilia occidentale è ospitato nei locali del SIA, presso l'Edificio 11 di viale delle Scienze, ed è supportato dal personale del Settore RHS del SIA.

Art. 2
Diffusione del Disciplinare

Il personale UNIPA verrà informato in merito all'adozione del presente Disciplinare tramite apposita circolare; lo stesso sarà disponibile sul Portale di UNIPA e affisso all'Albo d'Ateneo.
Il Disciplinare potrà essere aggiornato, alla luce dell'innovazione tecnologica, ogni qualvolta se ne ravvisi la necessità; di tali revisioni sarà data tempestiva comunicazione al personale nelle predette modalità.

Art. 3
Definizioni

Ai fini del presente disciplinare, si intende per:

• **"Rete di Ateneo"**, l'insieme di tutte le reti locali delle Strutture dell'Ateneo. La rete di Ateneo ha lo scopo di consentire la condivisione di risorse informatiche comuni, di veicolare il traffico "voce" tramite sistema VoIP-UNIPA e di permettere l'interscambio di informazioni e di ogni altra applicazione telematica all'interno e all'esterno dell'Ateneo;

. "**Rete GARR**", la rete italiana della ricerca gestita dal Consortium Garr (CNR, ENEA, INFN, CRUI, etc...);

• "**Sistema VoIP-UNIPA**", il sistema telefonico di Ateneo basato su tecnologia VoIP che utilizza la Rete di Ateneo per veicolare il traffico voce all'interno e all'esterno dell'Ateneo;

• **"Sistema Informativo di Ateneo (SIA)"**, il Servizio Speciale dedicato alle attività informatiche e telematiche inquadrato, amministrativamente, nell'ambito dell'Area Servizi a Rete;

• **"Utente",** qualsiasi soggetto a qualsiasi titolo autorizzato ad accedere alle risorse informatiche della rete dell'Ateneo di Palermo, ovvero:

1. Personale docente di ruolo
2. Personale ricercatore di ruolo
3. Personale TA (Tecnico/Amministrativo) a tempo indeterminato
4. Personale TA a tempo determinato
5. Docente supplente esterno
6. Collaboratore tecnico/amministrativo
7. Collaboratore alla didattica

8. Assegnista di ricerca
9. Docente a contratto
10. Docente dotato di dispositivo di firma digitale per la registrazione di. esami
11. Studente iscritto ai corsi di studio di 1° e 2° livello
12. Dottorando
13. Dottorando di Università consorziate
14. Studente di master
15. Laureato di un qualunque corso di studi/ dottorato/ master
16. Laureato di un qualunque corso di studi/ dottorato/ master titolare di una collaborazione a qualsiasi titolo
17. Ospite (convegnista, ospite occasionale, ...)
18. Personale di azienda esterna che svolge attività presso UNIPA (ad es.: AOUP, Fideliter, Sintesi, ARCA, Ersu, Comuni convenzionati per i servizi agli studenti, ..)
19. Personale di azienda/organizzazione esterna che fornisce servizi ICT a UNIPA (ad es: Selfin.it, CINECA, CILEA, ...) e AOUP (ad es.: Selfin.it, Siemens, Agfa, ...)
20. Personale in CdA e Senato Accademico (ad es: Studenti, ...)
21. Revisori dei Conti
22. Personale in quiescenza
23. Borsisti e studenti Erasmus

- **"Settore Gestione Reti, Hardware e Software (RHS)"**, è il settore del SIA preposto al sistema telematico di Ateneo, alla sicurezza informatica, ai sistemi di elaborazione dati centralizzati, ai servizi sistemistici web, e-mail e DNS (Domain Name Server), all'Identity Management, alla gestione sistemistica dei database, al backup/restore dei dati, alla gestione dei sistemi di BI&DR (Business Continuity e Disaster Recovery) secondo le indicazioni di DigitPA;
- "**Settore Logistica e Servizi Generali (LSG)"**, è il settore del SIA preposto al sistema VoIP-UNIPA, alla gestione degli Amministratori di Sistema (AdS) secondo i dettami del D.Lgs. 196/2003 e per la firma digitale associata al personale UNIPA, alla e-mail dedicata agli studenti su @community.unipa.it;
- "**Sistema personale**", è un sistema di elaborazione non condiviso con altri soggetti e che non eroga servizi accessibili ad altri (ad es. : PC, portatili, palmari, smartphone);
- "**Sistema multiutente**", è un sistema di elaborazione condiviso da più utenti (ad es.:*workstation, server*);
- "**Sistema Intranet**", è un sistema di elaborazione dedicato ad applicazioni Intranet (Server);
- "**Sistema Internet**", è un sistema di elaborazione dedicato ad applicazioni Internet (Server);
- "**Apparecchiature di rete**", dispositivi di rete *(hub, switch, router, access point)* o dispositivo di accesso remoto (*terminal server*) o dispositivo di comunicazione remota (telecamere, sistemi di video conferenza, modem);
- "**Posta elettronica**", scambio di messaggi e di *files* attraverso una rete locale o Internet.
- **Amministratore di Sistema (AdS)"**, è il soggetto, dall'Amministrazione universitaria appositamente designato con provvedimento formale, alla gestione e/o alla manutenzione di uno o più sistemi collegato/i alla Rete di Ateneo; con riferimento al Provvedimento del 27 Novembre 2008 del Garante Privacy sono da considerare, a tutti gli effetti AdS, i soggetti che, in via continuativa, svolgono operazioni di:

1) Amministrazione di Sistemi Informatici (System Administrator)
2) Amministrazione di Server (Server Administrator)
3) Amministrazione di Sistemi di Rete (Network Administrator)
4) Amministrazione di Sistemi di Sicurezza (Security Administrator)
5) Amministrazione di Software e Applicazioni (Application Administrator)
6) Amministrazione di Database (Database Administrator)

7) Amministrazione di Sistemi di Salvataggio Dati (Backup / Storage Administrator)
8) Amministrazione di Sistemi di Ripristino Dati (Recovery Administrator)
9) Amministrazione di Siti Web (Web Administrator)
10) Altri soggetti addetti alla gestione o alla manutenzione di strumenti elettronici che per l'espletamento delle loro funzioni devono compiere operazioni di amministrazione
11) Amministrazione di Apparati Hardware (Hardware Administrator).

La regolamentazione per l'accesso ai servizi di rete per l'Utente afferente agli Enti strumentali/convenzionati/consorziati con UNIPA sarà oggetto di apposite convenzioni con gli stessi. Nel caso in cui l'Ente convenzionato/consorziato/strumentale abbia la necessità di far accedere ai servizi di rete (WiFi, VPN, ..) un numero di utenze superiore a 30, l'autenticazione delle utenze e il supporto informatico alle stesse avverrà tramite dispositivi, collegati a quelli del SIA, e personale a cura dell'Ente stesso; la responsabilità sul riconoscimento dell'Utente è a cura dell'Ente strumentale/convenzionato/consorziato.

Art. 4
Rete di Ateneo. Modalità di accesso e di utilizzo

Accesso alla rete di Ateneo
L'accesso ad Internet dalla rete di Ateneo avviene attraverso la rete GARR e, pertanto, ogni Utente è tenuto all'accettazione integrale delle norme contenute nel documento "*Acceptable User Policy*" del GARR che è consultabile sul Portale UNIPA e su Internet.
L'accesso alla rete di Ateneo è consentito agli utenti previamente identificati a cui è stato attribuito un codice identificativo (*Userid, tipicamente nome.cognome*) e una parola chiave segreta (*Password*). Scelta, custodia, modifica e utilizzo della *password* devono rispettare le seguenti prescrizioni:

- la password viene attribuita e comunicata all'Utente dal personale afferente al Settore RHS del SIA.; al primo accesso e-mail via web, il sistema invita l'Utente a sostituirla con una a sua scelta; la password è strettamente personale e non va comunicata ad alcuno;
- la password deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'Utente (nome, cognome, data di nascita ecc..);
- l'Utente ha la responsabilità di custodire la propria password e non comunicarla ad altra persona;
- l'Utente è invitato dal sistema a cambiare la propria password su base almeno semestrale; nel caso di trattamento di dati sensibili e/o giudiziari, la periodicità della variazione è ridotta a tre mesi (come previsto dal punto 5 del Disciplinare tecnico - All. B - allegato al D. Lgs. 196/2003);
- l'Utente deve dare immediata informazione all'AdS nel caso in cui abbia fondato motivo di ritenere che possa essere compromessa la riservatezza della password o che ne sia stato fatto un utilizzo indebito.

Inoltre, l'Utente:

1. deve avere associato un indirizzo IP (in modalità statica o dinamica) e l'AdS della Struttura di riferimento (Facoltà, Dipartimento, Segreteria Studenti, Uffici amministrativi, aule didattiche, ...) deve essere in grado di associare l'indirizzo IP alla persona fisica che lo sta utilizzando per la propria stazione di lavoro; in mancanza di tale figura, l'associazione dovrà essere effettuata dal personale afferente al Settore RHS del SIA (il modulo "Richiesta registrazione nodo della Rete di Ateneo dell'Università di Palermo" è disponibile sul Portale UNIPA); ogni appropriazione indebita di indirizzo IP può dare luogo alla disabilitazione dell'accesso ai servizi di rete e alla

comunicazione da parte del personale SIA agli Organi competenti per la verifica di eventuali responsabilità disciplinari;
2. non può collegare apparecchiature alla rete universitaria senza il coinvolgimento dell'AdS di riferimento della Struttura o, in assenza di questi, al personale afferente al Settore RHS del SIA;
3. non deve utilizzare sistemi operativi obsoleti e/o inaffidabili collegati alla rete;
4. non deve utilizzare strumenti *software* e/o *hardware* atti a perpetrare illeciti informatici;
5. non deve cedere a persone non autorizzate e non lasciare incustodita la propria postazione, una volta superata la fase dell'autenticazione e/o dell'applicazione a cui si è avuto accesso.

E' vietato:
- fornire il servizio di connettività di rete a Utenti non autorizzati all'accesso alla rete;
- usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi (per esempio utilizzo di "Tunnel"); gli AdS e il personale del SIA possono impedire, in qualsiasi momento, l'accesso alla rete d'Ateneo da parte di Utenti anonimi o non identificati né da UNIPA né dagli Enti convenzionati/strumentali con UNIPA;
- non rispettare gli obblighi contrattualmente assunti dall'Università e la normativa di riferimento in materia di *copyright*, licenze d'uso di *software* e connettività di rete;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distraggano risorse (capacità di memorizzazione, capacità di elaborazione, ...), danneggino o riducano l'utilizzabilità o le prestazioni della rete;
- accedere senza autorizzazione, se richiesta, ad archivi e banche dati;
- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore;
- distruggere, danneggiare, intercettare o accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi; usare, intercettare o diffondere *password* o codici di accesso o chiavi crittografiche di altri utenti o di terzi e, in generale, commettere attività che violino la riservatezza di altri utenti o di terzi.

Inoltre valgono le seguenti regole relative all'utilizzo del personal computer e degli altri dispositivi elettronici in uso presso l'Università ad eccezione dei sistemi informatici dedicati alla ricerca.

1. I personal computer fissi e portatili acquisiti con fondi dell'Amministrazione e i programmi su di essi installati sono uno strumento di lavoro; contenendo anche dati e informazioni personali di terzi, detti strumenti devono essere utilizzati con diligenza e cura.
2. Le impostazioni dei personal computer, nonché l'installazione di sistemi operativi e programmi applicativi, avviene di norma con il supporto degli AdS sulla base di criteri e profili decisi dall'Amministrazione e seguendo i necessari criteri di sicurezza. In ogni caso, l'uso dei programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta fornite dall'Amministrazione.
3. Al termine delle attività di fine giornata che prevedono l'utilizzo della stazione di lavoro, questa deve essere spenta, assieme alle altre apparecchiature ad essa collegate (stampante, scanner, ..) prima di lasciare gli uffici.
4. Per finalità di assistenza, manutenzione e aggiornamento e previo avviso all'Utente, l'AdS può accedere da remoto alla stazione di lavoro dello stesso, nel rispetto della privacy.
5. Ciascun Utente deve prestare la massima attenzione nell'utilizzo di supporti di memorizzazione esterna (*dispositivi usb, ..)* e deve avvertire immediatamente l'AdS nel caso in cui vengano rilevati virus.

In quanto allo smaltimento di *hardware* non più utilizzabile, si richiama la circolare della Direzione Amministrativa del 18/12/2008, prot. 95911-I/6.

Uso di sistemi personali
E' consentito collegare alla rete di Ateneo sistemi di elaborazione che non sono di proprietà della Università (personal computer, portatili, palmari ecc.), purché vengano rispettate le prescrizioni indicate per i sistemi in uso presso l'Università, in particolare modo per quanto riguarda i sistemi di sicurezza.

Sistema multiutente
Il sistema multiutente è tipicamente un server che offre dei servizi a più utenti. Questo può essere installato in un qualsivoglia locale all'interno di UNIPA purché abbia un AdS di riferimento responsabile dei servizi erogati. Per ragioni di sicurezza informatica, se il server è allocato presso il SIA e non è indicato formalmente l'AdS di riferimento, il server verrà spento; se il server si trova presso struttura di Ateneo diversa dal SIA e non ha un AdS di riferimento non potrà essere raggiungibile da Internet.

Aggiunta di punti di rete
L'attivazione di ulteriori punti permanenti di accesso alla rete locale della struttura di appartenenza deve esser concordata con l'AdS della Struttura o, in assenza di questi, con il personale del SIA.

Rete VoIP
Non è consentito collegare alla rete di Ateneo apparecchiature di rete VoIP senza l'esplicita autorizzazione del Responsabile del Settore LSG del SIA.

Art. 5
Accesso in Internet

L'utilizzo della rete Internet è consentito per scopi didattici, di ricerca e per l'accesso a dati e informazioni concernenti l'attività istituzionale dell'Università degli studi di Palermo e degli enti convenzionati/strumentali. La navigazione avviene previo accesso al sistema "captive portal" installato presso il SIA utilizzando le credenziali di accesso associate a ciascun Utente. Il sistema in argomento consente l'accesso alle risorse Internet, svolge funzioni di antivirus per tutto il traffico di rete da/verso Internet che lo attraversa e svolge funzioni di firewall per la prevenzione di attacchi informatici. I log prodotti da questo sistema riguardano alert relativi a virus e attacchi informatici; relativamente alla navigazione web dei singoli utenti i log sono memorizzati secondo le indicazioni del D.Lgs. 196/2003 e possono essere visionati solo dall'Autorità Giudiziarie dopo formale richiesta. I log che risalgono ad un anno prima rispetto al giorno corrente verranno automaticamente cancellati.

Art. 6
E-mail

Gestione delle e-mail

Il personale del Settore RHS del SIA provvede ad attivare/disattivare per ciascun utente una e-mail personale e, per ogni Struttura, una o più e-mail di Struttura, con uno spazio disco assegnato sulla base della disponibilità in essere per la normale attività e per il backup.

L'attivazione di una e-mail è effettuata attraverso l'assegnazione di una username e della relativa *password*-iniziale.

Il personale di stanza al SIA non può esercitare visura, controllo, censura, modifica, cancellazione dei messaggi di posta elettronica ricevuti e inviati dagli Utenti, fatte salve le normali operazioni di intercettazione da parte di appositi filtri automatici di virus o spam contenuti nei messaggi stessi, ad

eccezione dei casi in cui ciò si renda necessario per adempiere ad una disposizione di legge, ad un ordine giudiziario o a disposizioni delle autorità di pubblica sicurezza.

Vengono memorizzati i dati di log standard di sistema, generati automaticamente per ciascuna e-mail, riguardanti: indirizzo e-mail del mittente, indirizzo e-mail del destinatario, indirizzo IP del server mittente, indirizzo IP del server destinatario, data ed ora, numero destinatari, dimensione in byte del messaggio, tempo impiegato per la consegna, stato consegna del messaggio. I log che risalgono ad un anno prima rispetto al giorno corrente verranno automaticamente cancellati.

Il personale afferente al Settore RHS del SIA non può divulgare in alcun modo i dati di log a meno che ciò non venga richiesto dalle autorità competenti, ovvero nel caso in cui ciò sia necessario per adempiere ad una disposizione di legge, ad un ordine giudiziario o ad una disposizione degli Organi di governo dell'Ateneo.

Compiti e responsabilità

1. L'Utente è responsabile della propria casella di posta elettronica personale; responsabile delle caselle di posta elettronica di Struttura é il Responsabile della Struttura; lo stesso ne può delegare la gestione indicando al SIA, per iscritto, il nominativo del delegato.
2. L'Utente è responsabile del proprio *userid*, della segretezza della relativa *password* e del contenuto dei messaggi inviati dalla propria casella; egli è responsabile di tutte le operazioni effettuate con la casella di posta elettronica relativa all'*userid* ad esso associato.
3. L'Utente è responsabile delle eventuali conseguenze pregiudizievoli che un uso improprio del servizio da parte del proprio *userid* potrebbe comportare a terze persone, e ciò in riferimento alla vigente normativa in materia civile e penale.
4. La *password* di accesso ai servizi di rete, compreso il servizio di posta elettronica, è strettamente personale ed in nessun caso va comunicata a terze persone, sia verbalmente che per iscritto. Qualora, per motivi tecnici, il personale del SIA, su richiesta dell'Utente, abbia necessità di conoscere la *password* di accesso ai servizi di rete, l'Utente deve cambiarla immediatamente dopo l'intervento tecnico.

Utilizzazione del servizio

1. Non inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
2. Non inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve procedere all'immediata cancellazione. Non si devono, in alcun caso, aprire e/o scaricare gli allegati di tali messaggi.
3. Limitatamente al rinnovo delle rappresentanze negli Organi Collegiali di Governo dell'Ateneo e del C.N.S.U., l'invio di messaggi per fini di comunicazioni elettorali è consentito su apposita autorizzazione del Direttore Amministrativo;
4. Non inviare lo stesso messaggio a più di 200 (duecento) destinatari. Laddove le Strutture avessero la necessità di inviare comunicazioni ad una pluralità di destinatari, deve essere usato il gestore delle *mailing list* disponibile su apposito server del SIA. L'utilizzo di tale server è consentito ai singoli Utenti solo dietro autorizzazione scritta e motivata da parte del responsabile della Struttura di appartenenza.
5. Non diffondere messaggi di provenienza dubbia.
6. Per la trasmissione di comunicazioni all'interno dell'Università dovrà essere privilegiato l'uso della e-mail (ai sensi dell'art. 33, comma 1 lett. m) L. 18 giugno 2009 n. 69), prestando attenzione alla

dimensione degli allegati (si richiama a tal proposito la Circolare del Direttore Amministrativo prot. n. 34731 del 18/05/2010 avente ad oggetto "comunicazioni mezzo e-mail").

7. In caso di assenza prolungata programmata, si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate (anche elettroniche o telefoniche) di un collega o della struttura di riferimento da contattare in sua assenza e/o altre modalità utili di contatto della struttura organizzativa presso cui presta la propria attività lavorativa.
8. Nell'ipotesi di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa l'interessato può delegare un altro utente ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'Area in cui presta servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere informato il dipendente interessato alla prima occasione utile.
   Al termine dell'esigenza verificatesi all'utente interessato è fatto obbligo modificare la password di accesso.
9. Qualora si verificassero anomalie nell'invio e ricezione dei messaggi di posta elettronica dovrà essere prontamente informato l'AdS.
10. Gli indirizzi di posta elettronica vengono mantenuti, di norma, fino a 18 mesi dopo la data di fine rapporto ad eccezione del personale docente in quiescenza che mantiene il diritto compreso accesso VPN; un sistema automatico, in caso di inattività prolungata di almeno 180 gg., cancellerà dai sistemi l'utenza e la relativa e-mail con tutti i messaggi memorizzati.

Art. 7
Accesso in VPN (Virtual Private Network)

Il servizio VPN, tramite accreditamento attraverso le proprie credenziali di accesso (username e password), permette l'accesso ai servizi universitari erogati via web (contabilità, protocollo, etc.). Gli studenti e il personale universitario inoltre potranno accedere ai servizi offerti dallo SBA (Servizio Bibliotecario di Ateneo). In modalità VPN non è consentita, di norma, la normale navigazione su Internet.

Art. 8
Accesso tramite il servizio WiFI

Le utenze personali sono abilitate ad utilizzare il servizio WiFI per accedere ai servizi universitari erogati via web e a Internet; gli AdS devono vigilare sulla presenza di altri SSID (Service Set IDentifier) universitari che operano in conflitto con quelli implementati dal personale afferente al Settore RHS del SIA e aiutano l'utenza di riferimento (studenti, personale universitario, ...) a configurare la connessione in rete. Sul Portale UNIPA è disponibile la documentazione necessaria alla connessione e relativa ai più diffusi sistemi operativi per PC e palmari. Si ricorda che presso il SIA non si offre supporto diretto agli Utenti.

Art. 9
Misure minime di protezione e sicurezza

L'applicazione di filtri a livello di *router/firewall* consente di mantenere basso il rischio di attacchi informatici da/verso Internet e verso i sistemi di elaborazione del SIA; il personale afferente al Settore RHS del SIA, seguendo anche le indicazioni del GARR, adotta regole e filtri sulla base delle diverse esigenze/necessità operative di UNIPA e di ciascun Utente mantenendo basso il rischio di perdita di dati e appropriazione di identità informatica.

Art. 10
Mailing List

Il personale del Settore RHS del SIA mette a disposizione delle strutture che ne facciano richiesta un server dedicato alla gestione di *mailing list*. Tale server va utilizzato per la spedizione di messaggi di posta elettronica diretti a più di 200 (duecento) destinatari.
Le strutture che abbiano la necessità di effettuare tali spedizioni debbono richiedere al Responsabile del Settore RHS del SIA l'attivazione di un'apposita *mailing list*, specificando nome, cognome ed indirizzo *e-mail* dell'amministratore della lista, il quale è responsabile del corretto utilizzo della stessa, autorizzando le spedizioni ritenute opportune e scartando quelle ritenute non opportune.
L'elenco dei destinatari facenti capo alla *mailing list* è di pertinenza della struttura richiedente e va aggiornato dall'amministratore della lista.
Al fine di non intasare le caselle di posta elettronica dei destinatari e di non sovraccaricare i *server* dedicati al servizio di posta elettronica, eventuali allegati devono essere inviati nella forma di "Collegamento" e non inclusi nel corpo del messaggio.

Art. 11
Telefonia VoIP

Il settore del SIA preposto alla gestione del sistema telefonico di Ateneo è il Settore Logistica e Servizi generali del SIA. I log registrati prevedono la cancellazione degli ultimi tre numeri, nel caso di chiamate esterne al sistema VoIP, e il numero di secondi relativi alla conversazione tra chiamante e chiamato e ciò solo per fini di fatturazione trimestrale all'ufficio/struttura competente. I log che risalgono a 180 gg. prima rispetto al giorno corrente verranno automaticamente cancellati. Gli stessi log possono essere trattati per fini diversi alla fatturazione solo da parte delle autorità giudiziarie, dopo formale richiesta.

Art. 12
Disattivazione dell'accesso ai servizi di rete

L'accesso ai servizi di rete è concesso a tutti gli Utenti che si occupano di didattica e ricerca, anche dopo il pensionamento. Per tutti gli altri Utenti UNIPA, la disattivazione avverrà dopo 18 mesi dalla data di pensionamento (Personale, ..) o della scadenza del contratto (Docente a contratto, ...) o di status di studente (laureato, dottorato, assegnista, ...). Per gli Utenti afferenti agli Enti strumentali/convenzionati la disattivazione avverrà allo scadere della convenzione a cura dell'Ente se il relativo sistema di Identity Management è collegato informaticamente a quello del SIA.
In tutti i suindicati casi, un sistema automatico verificherà l'utilizzo dei servizi (e-mail, VPN, WiFi, ...) e disattiverà l'utenza dopo 6 mesi di inattività.

Art. 13
Controlli sull'osservanza del disciplinare

1. Per garantire la funzionalità e la sicurezza del sistema informatico, l'Università degli Studi di Palermo, nel rispetto dello Statuto dei lavoratori (art. 4 comma 2) si riserva di effettuare controlli c.d. 'indiretti' per accertare l'osservanza del presente disciplinare. Rispetto a tali controlli lo stesso costituisce preventiva e completa informazione nei confronti degli Utenti.

2. Gli eventuali controlli, generali ed estesi, atti a individuare condotte non conformi al presente disciplinare, avverranno preliminarmente su dati aggregati (c.d. "controllo anonimo") riferiti all'intera struttura lavorativa ovvero all'Area o al Settore. Qualora venissero rilevate anomalie o irregolarità, potrà essere inviato un avviso generalizzato all'utenza che richiami all'utilizzo corretto degli strumenti elettronici d'Ateneo, nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
3. Qualora le anomalie o le irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente all'Ufficio in cui è stata rilevata l'anomalia. In caso di ulteriori, ripetute e significative anomalie o irregolarità (rilevate, ad esempio, per la presenza di virus provenienti da siti non istituzionali), si procederà ad ulteriori controlli al fine di individuare le eventuali responsabilità personali.
4. Qualora venisse constatata la violazione del presente disciplinare, l'Università degli Studi di Palermo potrà irrogare le sanzioni previste dalle vigenti diverse normative di riferimento, a seconda della tipologia di utenza universitaria, e/o attivare i relativi procedimenti.
5. Oltre a tali controlli di carattere generale, l'Università degli Studi di Palermo si riserva comunque la facoltà di effettuare specifici controlli *ad hoc* nel caso di segnalazione di attività che hanno causato danno all'Amministrazione, che ledono diritti di terzi o che sono, comunque, illecite.

Art. 14
Violazioni e sanzioni

L'Utente è tenuto al rispetto del presente disciplinare.
La non osservanza di quanto sopra può comportare la restrizione o la revoca delle autorizzazioni ad accedere alla rete di Ateneo; il personale del SIA, valutata la gravità dell'eventuale illecito, provvede ad istruire la relativa pratica e a trasmetterla agli Organi competenti di Ateneo.

Art. 15
Norme finali

Per quanto non espressamente previsto dal presente Disciplinare, si rinvia alle norme di Legge, allo Statuto e ai Regolamenti dell'Università degli Studi di Palermo e alle norme di utilizzo della rete emanate dal C*onsortium* GARR. „

Il Rettore
Prof. Roberto Lagalla