UNIVERSITÀ DEGLI STUDI DI PALERMO

IL RETTORE

VISTO lo Statuto dell'Università degli Studi di Palermo;
VISTA la delibera n. 08/01 del 17 dicembre 2019 del Senato Accademico;
VISTA la delibera n. 08/01 del 18 dicembre 2019 del Consiglio di Amministrazione;

DECRETA

di emanare il

"REGOLAMENTO SULL'UTILIZZO DELLA RETE DI ATENEO E DEI SERVIZI INTERNET"

Art. 1 Principi generali

1. Il presente regolamento ha per oggetto i principi, i criteri e le modalità operative generali che concorrono all'accesso e utilizzo degli strumenti informatici aziendali della rete di Ateneo e dei servizi Internet da parte degli operatori e del personale dell'Università degli Studi di Palermo, denominata d'ora innanzi UNIPA, con particolare riferimento agli aspetti connessi alla tutela dei dati in essi presenti ed alla salvaguardia dei dispositivi informatici.
2. Al fine di mantenere Il presente documento sempre conforme alle norme, le modalità operative dei servizi di rete verranno demandate ad apposite Linee guida dei Servizi in rete (d'ora in avanti "Linee guida") che, alla luce dell'innovazione tecnologica e ogni qualvolta se ne ravvisi la necessità, saranno oggetto di aggiornamento periodico da parte del Responsabile della Transizione al digitale, sentiti il Responsabile per la Protezione dei dati personali (RPD) d'Ateneo per gli aspetti connessi alla privacy e il Delegato del Rettore ai Servizi Informativi d'Ateneo, al fine di garantirne l'efficacia applicativa e l'attualità; tali Linee Guida verranno adeguatamente diffuse tra tutto il personale dell'Università e saranno disponibili sul Portale di UNIPA. Le relative variazioni saranno divulgate tramite apposita circolare e pubblicate nell'area intranet.

Parte I – Infrastrutture di rete

Art. 2 Rete di Ateneo

1. Si definisce "rete di Ateneo" l'insieme di tutte le infrastrutture passive, interconnesse attraverso apparati attivi, finalizzato a consentire la condivisione delle risorse informatiche comuni e l'interscambio dei dati e delle informazioni tra le applicazioni telematiche, sia all'interno che all'esterno dell'Ateneo.
2. La rete di Ateneo è articolata sul territorio metropolitano e sui poli didattici di Agrigento, Caltanissetta e Trapani, e si interconnette ad Internet attraverso l'infrastruttura di rete per l'Università e la Ricerca gestita dal "Consortium GARR – Gruppo Armonizzazione Reti della Ricerca" (CNR, ENEA, INFN, CRUI, etc...).
3. Il nodo GARR per la Sicilia occidentale è ospitato nei locali dell'Area Sistemi informativi e portale di Ateneo (SIA), presso l'Edificio 11 di viale delle Scienze, ed è supportato dal personale del Settore Servizi Generali Informatici di Ateneo (di seguito denominato Settore) preposto come indicato nelle Linee guida.

Art. 3 Apparati attivi

1. Nell'infrastruttura di rete di UNIPA gli apparati attivi, router, switch, access point, etc. di proprietà dell'Ateneo e inventariati dai vari centri di costo devono essere istallati sulla base di uno specifico progetto esecutivo redatto dalla struttura interessata e su indicazione del Settore preposto. Ogni apparato deve essere registrato su un apposito sistema di registro informatico insieme ai dati necessari per la sua individuazione nella topologia del network e all'indicazione del personale di riferimento da contattare in caso di guasto o disservizio.

Art. 4 Dispositivi e strumenti informatici

1. Alla rete di Ateneo vengono interconnessi gli strumenti informatici: personal computer, notebook, tablet, smartphone, che usufruiscono dei servizi di rete messi a disposizione dai server, consentendo l'interscambio dei dati degli applicativi software installati. Tutti i dispositivi e gli strumenti informatici devono essere individuati all'interno della rete tramite l'utenza che ne assume la responsabilità.
2. Le modalità di utilizzo dei dispositivi informatici sono regolamentate dalle Linee guida dei servizi in rete.

Art. 5 Monitoraggio e misure minime di protezione e sicurezza

1. La rete di Ateneo è una struttura complessa e, pertanto, è necessario individuare e definire eventuali sottosistemi tecnici e/o organizzativi omogenei al fine di applicare le misure più adatte per contrastare i rischi legati alle minacce alla sicurezza informatica.
2. E' consentito l'accesso alla rete di Ateneo solo ai dispositivi autorizzati con modalità specificate nelle Linee guida.
3. E' necessario, inoltre, proteggere le configurazioni hardware e software degli apparati e dei dispositivi verificandone, periodicamente, l'integrità e la vulnerabilità.
4. Per mantenere basso il rischio di attacchi informatici da/verso Internet e verso i sistemi di elaborazione nel Centro elaborazione dati **(**CED**)** del SIA, è consentito l'uso, nel rispetto della vigente normativa di settore, di sistemi di analisi dei log del traffico dati, correlati a blacklist dei sistemi di certificazione digitale **(**CERT**)** e agli elementi attivi collezionati tramite sistemi Intrusion Prevention System (IPS).
5. Tutto il personale incaricato della gestione della rete e dei sistemi informatici, seguendo le indicazioni del GARR e del Settore preposto, deve adottare regole e profili adeguati alle diverse esigenze/necessità operative della struttura e delle tipologie di utenza autorizzata. Le suddette regole e profili consentiranno di rendere operativa l'applicazione delle misure minime di sicurezza previste dalla vigente normativa di settore e mantenere basso il rischio di perdita di dati e di appropriazione di identità informatica, così come previsto dalle Linee Guida.

Parte II – Servizio di Identity Management di Ateneo

Art. 6 Identity Management

1. L'Ateneo è dotato di un sistema di Identity Management centralizzato e **mantiene** popolata la sua anagrafica attraverso modelli di estrazione e correlazione dei dati ottenuti dalle banche dati di riferimento (CSA, UGOV, GEDAS, etc).
2. Il servizio di Identity Management gestisce e garantisce l'identità elettronica di persone fisiche e deve essere conforme alle norme e agli accordi con la federazione Identity Management (IDEM) attraverso il DOPAU (DOcumento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione).
3. In ottemperanza alle norme introdotte con il regolamento europeo sulla protezione dei dati, ai fini della certificazione della comunicazione, i sistemi informatici rilasciano credenziali identificatrici, personali ed incedibili, relativamente ad identità digitali di persone fisiche; per tali motivi il servizio di Identity Management può rilasciare credenziali riferite a persone giuridiche o a strutture interne all'Ateneo a condizione che vengano riferite a un Responsabile interno dell'Ateneo.
4. Il servizio di Identity Management deve essere compatibile con il Sistema Pubblico di Identità Digitale (SPiD) e prevedere, eventualmente, il riconoscimento del cittadino per particolari servizi disponibili in rete attraverso il web.
5. Ad ogni persona fisica che intrattiene, a vario titolo, un rapporto giuridico con l'Università degli Studi di Palermo (studente, professore, personale tecnico amministrativo, collaboratore, ospite, etc.), deve essere attribuita una propria identità digitale.

6. L'Utente di Ateneo accetta di essere riconosciuto quale responsabile delle attività espletate in rete e sui dispositivi informatici tramite la propria identità digitale.
7. L'Utente si impegna, inoltre, ad adoperarsi attivamente per salvaguardare la riservatezza della sua password, a segnalare qualunque situazione che possa inficiarla ed a modificarla sulla base dei requisiti minimi di sicurezza.
8. Al fine di garantire l'identità digitale degli utenti di Ateneo e ridurre i livelli di rischio dovuti ad una eventuale sostituzione di persona, tutti gli applicativi web che richiedono il riconoscimento dell'utente devono essere adeguati alle specifiche tecniche definite dal servizio di Identity Management, così come previsto dalle Linee Guida.

Art. 7 Ruoli e Autorizzazione

1. Il ruolo è la definizione della posizione in funzione del compito da svolgere all'interno dell'Ateneo.
2. Il servizio di Identity Management deve definire, per ogni utenza, tutti i livelli di autorizzazione relativamente all'accesso e alla gestione dei servizi e degli applicativi operanti nella rete di Ateneo; tali livelli sono assegnati in accordo ai ruoli dell'utente e definiti dalle fonti autorizzative di Ateneo.
3. Ogni servizio in rete dovrà essere censito e, affinché l'utente possa fruire del predetto servizio, dovranno essere definiti i ruoli e i relativi livelli di autorizzazione.
4. I ruoli devono essere mappati, gestiti e assegnati all'utenza attraverso un apposito sistema informatico centralizzato di Ateneo.
5. La perdita di un ruolo, da parte dell'utente, comporta la revoca immediata delle relative autorizzazioni su tutti i servizi in rete definite sul ruolo specifico con la sola eccezione della posta elettronica che viene mantenuta per ulteriori 12 mesi.

Art. 8 Credenziali per accounting di servizio

1. E' possibile creare particolari servizi e permettere un accounting temporalmente definito a gruppi di utenza non registrata nelle fonti autoritative di Ateneo come ospiti, convegnisti, personale di aziende esterne, etc.
2. Tali servizi devono prevedere gli accorgimenti necessari alla generazione dei log secondo le vigenti norme, opportuni processi di identificazione certa del soggetto utilizzatore sia del servizio che della connessione in rete e degli accessi in internet, sistemi di network isolation per ridurre il rischio di spoofing, broker e shared intercept.
3. Le credenziali per l'utenza non registrata nelle fonti autoritative di Ateneo dovranno essere, in ogni caso, rilasciate in modo automatico a seguito di una registrazione o una comprovazione in delega (ai sensi del successivo art.21) dell'identità della persona fisica.
4. Tutti i sistemi con accounting di servizio dovranno essere elencati su apposito sistema di registro elettronico.

Art. 9 Sicurezza delle credenziali

1. Scelta, custodia, modifica e utilizzo della password devono rispettare le prescrizioni previste dal servizio Rilascio Credenziali, secondo quanto previsto dalle Linee guida.
2. La password è strettamente personale e non va comunicata ad alcuno in quanto, in virtù delle credenziali uniche di Ateneo, si avrebbe accesso ad applicativi in base al ruolo e alle autorizzazioni assegnate all'utente.
3. L'Utente, nel caso in cui abbia fondato motivo di ritenere che possa essere compromessa la riservatezza della propria password o che ne sia stato fatto un utilizzo indebito, è tenuto a dare immediata informazione all'Amministratore di Sistema (di seguito AdS) di riferimento e al Settore preposto (indicare indirizzo mail di riferimento).
4. Per servizi ad alto rischio di data breach deve essere utilizzato il sistema di autenticazione a più fattori.

5. E' fatto divieto all'utente di accedere, in modo non autorizzato, tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti, ad alcuno dei servizi di Ateneo, ad altri account o a sistemi o reti interconnesse.

Art. 10 Registri di Sicurezza

1. In ottemperanza alle direttive del Regolamento Generale sulla Protezione dei Dati (di seguito GDPR) e secondo quanto disposto dalla vigente normativa di settore per la valutazione del rischio di sicurezza informatica, il Settore preposto è tenuto a mantenere un'opportuna standardizzazione della topologia del network di Ateneo, individuando le componenti di apparati attivi e passivi e le componenti dei dispositivi attivi personali e/o atti alla realizzazione dei servizi fruiti in rete.
2. E' consentita l'implementazione dei registri di sicurezza che correlano tutte le informazioni necessarie ad istruire, implementare e gestire attivamente le configurazioni di sicurezza relative a laptop, server e workstation, in modo da monitorare eventuali attacchi sulle vulnerabilità dei servizi e delle configurazioni e correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
3. I registri dovranno raccogliere e organizzare i dati relativi ai servizi in rete, identificare i ruoli di accesso e utilizzo da parte dei titolari e definire l'inventario delle utenze amministrative con riferimento ai privilegi e ai profili di accesso. Tali registri verranno implementati secondo le specifiche tecniche contenute nelle Linee guida.
4. Al fine di controllare l'istallazione, la diffusione e l'esecuzione di codice maligno (malware) è consentita l'istallazione di agent client in diversi punti della rete e il controllo degli apparati ad alto rischio informatico. E', inoltre, necessario definire un inventario delle configurazioni dei sistemi di sicurezza locali e perimetrali di Ateneo (firewall, IPS) al fine di monitorare attivamente i protocolli esposti e le autorizzazioni di accesso ai servizi e alla navigazione Internet. Ciò in modo da mitigare i possibili effetti di accessi a protocolli lasciati aperti per obsolescenza nell'uso dei servizi.
5. Attraverso il sistema dei registri di sicurezza è necessario effettuare un controllo applicativo sul traffico generato e poter valutare l'isolamento delle reti consentendo il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

Parte III – Uso e connessione alla rete

Art. 11 Uso della rete

1. L'uso della rete di Ateneo è finalizzato agli scopi di didattica, di ricerca, di terza missione e allo svolgimento delle attività istituzionali dell'Università degli Studi di Palermo.
2. L'integrità della rete d'Ateneo deve essere scrupolosamente protetta da appositi dispositivi di sicurezza informatica (firewall, idp, antivirus, ecc.).
3. Alla rete universitaria non può essere collegato alcun apparato informatico non identificato senza il coinvolgimento degli Amministratori di sistema (AdS) di riferimento della Struttura e/o del personale afferente al Settore preposto in accordo all'art.3, 4 del presente regolamento.
4. Tutti gli utenti della rete d'Ateneo, al fine di garantire le misure di sicurezza previste dalla normativa di settore, devono attenersi alle regole di comportamento previste dalle Linee guida.
5. Gli AdS e il personale del Settore preposto possono impedire, in qualsiasi momento, l'accesso alla rete d'Ateneo da parte di utenti anonimi o non identificati da UNIPA
6. Sulla base delle comunicazioni del GARR o del monitoraggio effettuato da parte del personale del Settore preposto, l'accesso alla rete d'Ateneo può essere revocato a ogni utente fino alla risoluzione dell'eventuale problema di sicurezza sui propri apparati.

Art. 12 Connessione alla rete e connessioni applicative

1. L'accesso dei sistemi attivi alla rete d'Ateneo avviene attraverso la loro connessione wired o wireless agli apparati attivi del network su protocolli TCP/UDP e IP.
2. E' compito degli Amministratori di sistema (AdS) di riferimento della Struttura garantire all'utente la corretta connessione del proprio apparato alla rete locale, registrando su apposito sistema i dati dell'apparato, l'utente responsabile, i dati di rete ed eventuali specifiche particolari (porte di connessioni, servizi) necessari alla corretta fruizione del servizio.
3. E' compito degli amministratori di sistema (AdS) di riferimento della Struttura provvedere alla mappatura IP di tutti gli apparati e alla gestione della topologia della propria sottorete secondo quanto previsto nelle Linee guida, in accordo con il Settore preposto.
4. Specifiche connessioni su altri protocolli e/o su porte non standard possono essere effettuate in accordo con il personale del Settore preposto, ove non ci siano incompatibilità e/o interazioni che limitino le comuni attività istituzionali.
5. Sono consentite connessioni a basso, medio e alto livello applicativo, come VLAN, dominio o installazione di applicativi che consentono il controllo remoto di altri sistemi; tali connessioni sono consentite sempre nel rispetto delle misure di sicurezza informatiche e della salvaguardia dell'integrità degli stessi sistemi.
6. Non sono consentite connessioni dirette a nodi distribuiti come peer-to-peer, se utilizzate per il trasferimento di materiale in violazione delle norme sulla proprietà intellettuale.
7. Per motivi didattici e/o di ricerca, eventuali implementazioni di connessioni particolari devono essere autorizzate dal Settore preposto e sviluppate utilizzando gli opportuni protocolli di sicurezza.
8. La tipologia di tali connessioni e le porte di rete utilizzate dovranno essere censite sul sistema di registro informatico; la piena responsabilità rimane in capo al richiedente, mentre l'AdS ha il compito di monitorare il corretto uso della connessione e dei servizi applicativi istallati.
9. Non sono consentite, se non espressamente autorizzate, connessioni ad apparati attivi che permettono di estendere la rete ad altre reti fuori dall'Ateneo e/o che facciano da gateway verso connessioni ad accesso Internet non opportunamente controllate.
10. Non sono consentite, se non espressamente autorizzate, connessioni specifiche su porte non standard sui sistemi firewall di frontiera di Ateneo.
11. La necessità dell'uso di porte non standard comporterà l'apertura di tutte le porte per l'IP specifico con conseguente responsabilità in capo al richiedente. Sarà onere dell'AdS mettere in sicurezza il relativo sistema attraverso l'opportuna configurazione di un firewall locale secondo le specifiche contenute nelle Linee guida.
12. Non è consentito generalmente, nella topologia della rete d'Ateneo, l'uso di sotto reti private non ruotabili o l'uso di servizi di NAT e Proxy. Tali soluzioni devono essere espressamente autorizzate definendo esplicitamente le responsabilità sui log e sulla tracciabilità dell'uso della sottorete come descritto dalle Linee guida.
13. E' compito del Settore preposto attuare tutte le strategie, secondo la normativa vigente, per mantenere una topologia della rete d'Ateneo sempre corrispondente alla realtà. Il Settore preposto deve essere in grado di rilevare le anomalie di funzionamento e garantire il funzionamento, informando contestualmente sia gli AdS che i titolari/responsabili sulle nuove tecnologie e i rischi rilevati, connessi all'implementazione di nuovi applicativi sui sistemi.

Art. 13 La connessione di aule e laboratori informatici

1. Le aule e i laboratori informatici sono sotto la diretta responsabilità degli AdS di riferimento e, di norma, sono collegati alla rete d'Ateneo in modalità wired con rilascio IP dinamico tramite DHCP locale o IP assegnato staticamente, secondo quanto descritto dalle Linee guida.

Art. 14 Servizi di rete

1. I servizi di rete sono fruiti da tutti gli utenti profilati dal sistema centralizzato di identity Management in funzione del proprio ruolo o profilati direttamente dal servizio di rete stesso in accordo con quanto detto sugli accounting di servizio.
2. La profilatura degli utenti sul sistema centralizzato di identity Management riguarda il personale strutturato, gli studenti dell'Ateneo e altro personale di volta in volta coinvolto nelle attività dell'Ateneo.
3. I servizi di comunicazione verso l'esterno devono essere utilizzati esclusivamente dal personale strutturato dell'Ateneo, dai dottorandi, specializzandi e assegnisti di ricerca, con carriera giuridicamente attiva.
4. L'accesso in relazione ad ogni servizio deve essere inibito in automatico al termine del periodo temporale di autorizzazione al ruolo e potrà essere cessato, dopo la data istituzionale di fine rapporto con l'Ateneo, se vengono superati i 6 mesi di inattività dall'ultimo uso.

Art. 15 Accesso in Internet

1. 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 (indicare URL).
2. L'Ateneo definisce i criteri e le modalità operative di accesso e utilizzo del servizio Internet da parte degli utenti autorizzati, in qualsiasi momento, le proprie politiche di sicurezza in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità.
3. 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.
4. L'utente può accedere a Internet per perseguire scopi strettamente personali non vietati dalla legge e per ragioni di lavoro al fine di raggiungere obiettivi di studio, ricerca e documentazione in relazione alle specifiche mansioni e alle specifiche competenze attribuite all'interno dell'Ateneo.
5. UNIPA può adottare modalità finalizzate a bloccare l'accesso a siti ritenuti non consoni allo svolgimento dell'attività lavorativa e/o comunque non affidabili. Può, altresì, definire la modalità di accesso ad Internet attraverso l'utilizzo di "whitelist" e "blacklist" adattivi attraverso analisi dei flussi di traffico e della "Reputation" degli IP contattati.
6. Le modalità operative e comportamentali da parte delle utenze per l'accesso a internet, al fine di garantire l'integrità di tutto il sistema informatico, sono descritte nelle Linee guida.
7. L'utente, in nessun caso, deve, di sua iniziativa, cercare di eludere le protezioni e/o il blocco alla connessione internet operato dai sistemi di sicurezza di Ateneo.
8. L'utente che fornisce a soggetti non autorizzati l'accesso alla connessione Internet, cedendo il proprio IP o inserendo le proprie credenziali sul sistema di captive portal, si assume la piena responsabilità delle operazioni condotte e protratte in rete dal soggetto.
9. L'utilizzo del servizio di accesso ad Internet termina d'ufficio allorché venga meno la condizione di utente autorizzato, non venga confermata l'autorizzazione d'uso, oppure questa venga revocata a seguito di accertamento diretto di attività non consentita o su segnalazione dell'autorità giudiziaria.
10. Il Settore preposto ha il compito, nel rispetto della normativa vigente e delle indicazioni dell'Autorità Garante per la protezione dei dati personali, di attuare tutte le strategie e utilizzare le tecnologie disponibili per minimizzare il rischio di attacco informatico attraverso la navigazione, implementando un sistema di sicurezza che consenta l'accesso alle risorse Internet analizzando le tipologie di traffico sui diversi protocolli da/verso Internet al fine di prevenire attacchi informatici, bloccando automaticamente le sorgenti esterne o interne di attacco.

Parte IV – Sistemi di comunicazione

Art. 16 Sistemi di comunicazione sincrona e asincrona

1. L'Ateneo, attraverso il Settore preposto, mette a disposizione servizi di comunicazione sincrona e asincrona al fine di aumentare lo scambio di informazioni necessarie allo svolgimento delle attività istituzionali, di divulgazione scientifica, di marketing, etc., da e verso le diverse tipologie di utenze.
2. Indicazioni sull'implementazione, le caratteristiche, l'uso e le responsabilità dei servizi di comunicazione sono contenute all'interno delle Linee Guida.

Art. 17 Sistemi di comunicazione istituzionali e di gruppo

1. Tutti i servizi implementati di comunicazione sincrona e asincrona possono essere istituzionali e di gruppo. I sistemi di comunicazione istituzionali sono di interesse generale per l'Ateneo e sono resi disponibili per tutte le tipologie e/o ruoli di utenti previste dalle politiche di autenticazione e autorizzazione specifiche per il servizio stesso.
2. Gli utenti abilitati ai servizi di comunicazione istituzionale sono tenuti ad usarli in modo congruo e sono responsabili in modo esclusivo sia del contenuto delle informazioni veicolate, che delle modalità di utilizzo del servizio stesso.
3. Per particolari scopi istituzionali di interesse non generale o per altri scopi non istituzionali, ma legati ad attività che coinvolgono giuridicamente l'Ateneo e/o gli uffici dello stesso, possono essere richieste e implementati servizi per la comunicazione di gruppo.
4. Gli utenti sono abilitati ai servizi di comunicazione di gruppo su proprio consenso, o in modo implicito se trattasi di servizi a supporto delle proprie attività lavorative di ufficio.
5. I servizi di comunicazione di gruppo hanno validità annuale e, se non espressamente rinnovati, dovranno essere sospesi e cessati dopo 90 giorni dalla sospensione.

Art. 18 Evidenza, obblighi e responsabilità per i sistemi di comunicazione

1. L'elenco dei servizi di comunicazione sincrona o asincrona, istituzionale e di gruppo dev'essere pubblicato su apposita sezione del sito web istituzionale e in esso devono essere espressamente individuati, per ogni servizio, l'ufficio e/o il responsabile. Devono, inoltre, essere definiti i parametri di gestione e monitoraggio degli accessi e dell'uso.
2. In osservanza alle norme vigenti ogni servizio deve garantire l'individualità dell'utilizzatore, la sua unicità e la relativa sicurezza informatica. Al fine di prevenire abusi, il servizio deve permettere il monitoraggio dei flussi dei dati per l'individuazione statistica di eventuali anomalie.
3. L'Università, in ottemperanza alle vigenti normative in materia di protezione dei dati personali, si impegna ad utilizzare i dati personali dell'utente ai soli fini dell'erogazione e della gestione dei servizi e di attuare quanto in suo potere per proteggere la riservatezza dell'utente medesimo.
4. L'Università si impegna, altresì, a fornire i servizi in modo continuativo secondo i Service Level Agreement (SLA) definiti nelle Linee Guida in relazione allo specifico servizio, fatte salve eventuali sospensioni dovute all'ordinaria o straordinaria manutenzione, a malfunzionamenti e ad eventi imprevisti ed imprevedibili.
5. L'Università attuerà tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita delle informazioni; ciò nonostante l'utente solleva l'Università da ogni responsabilità ed obbligazione relativa alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione delle comunicazioni o di altri contenuti, derivanti da guasti e/o malfunzionamenti degli apparati di gestione e, in generale, dall'erogazione del servizio stesso.
6. L'utente fruitore attivo dei servizi è responsabile del contenuto della comunicazione e di tutte le operazioni effettuate utilizzando il relativo sistema di comunicazione.
7. L'utente si impegna, nei confronti dell'Ateneo, a non utilizzare i servizi per scopi illegali o non conformi al presente regolamento o che comunque possano recar danno o pregiudizio all'Università medesima o a terzi.
8. L'utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio dei servizi, esonerando, contestualmente, l'Università da ogni

pretesa o azione che dovesse essere rivolta all'Università medesima da qualunque soggetto terzo, in conseguenza di tale uso improprio.

9. L'utente, inoltre, non può utilizzare i servizi di comunicazione in modo da danneggiare, disattivare, sovraccaricare, pregiudicare il servizio, o interferire con l'utilizzo e il godimento del servizio da parte degli altri utenti.
10. L'utente, salvo giustificabili eccezioni di cui comunque risponde personalmente, non può utilizzare i sistemi di comunicazioni per veicolare contenuti che contengano o rimandino a:
    - pubblicità non istituzionale, manifesta o occulta;
    - comunicazioni commerciali private;
    - materiale pornografico o simile, in particolare in violazione della Legge n. 269 del 1998 "Norme contro lo sfruttamento sessuale dei minori degli anni 18;
    - materiale discriminante o lesivo in relazione a razza, sesso, religione e altri fattori di discriminazione;
    - materiale che violi la normativa sulla privacy;
    - contenuti o materiali che violino i diritti di proprietà intellettuale, industriale, ecc… di terzi;
    - contenuti diffamatori o palesemente offensivi;
    - altri contenuti illegali.

    L'elenco che precede è da intendersi esemplificativo e non esaustivo.
11. In nessun caso l'utente potrà utilizzare i sistemi di comunicazione per diffondere codici dannosi per i computer quali virus e simili.
12. L'Utente si impegna, altresì, a non divulgare comunicazioni di natura ripetitiva (c.d. "catene di S. Antonio") anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).
13. L'Università si riserva la facoltà di segnalare alle autorità competenti, per gli opportuni accertamenti e i provvedimenti del caso, le eventuali violazioni alle presenti condizioni di utilizzo.
14. In caso di rilevazione di minaccia l'utente potrà essere inibito, senza preavviso e per il tempo necessario, all'uso attivo dei servizi di comunicazione. Inoltre, il servizio di gruppo stesso può essere sospeso anticipatamente fino alla risoluzione del problema.
15. Qualora si verificassero anomalie nella funzionalità dei servizi di comunicazione, dev'essere prontamente investito dell'accaduto l'AdS della struttura di appartenenza, il quale deve dare immediata comunicazione dell'anomalia al Settore preposto attraverso i canali di supporto messi a disposizione per la gestione del relativo servizio.

Art. 19 Installazione di Sistemi Server

1. Nel caso in cui alla rete di Ateneo vengano connessi sistemi server che forniscono servizi in rete a più strutture di UNIPA o servizi pubblici fruibili da internet, l'installazione dei suddetti sistemi deve avvenire esclusivamente presso il CED d'Ateneo ad opera del personale del Settore preposto e/o di altro personale autorizzato.
2. I sistemi dovranno essere registrati sul registro di sicurezza, insieme a tutti i dati necessari per la profilazione delle configurazioni e delle autorizzazioni in rete, e dovranno essere assegnati ad un AdS di riferimento, il quale dovrà gestire tutte le procedure per garantire la sicurezza del sistema e della rete.
3. Per motivi didattici, istituzionali e/o di ricerca è possibile, su espressa autorizzazione e su progetto esecutivo, istallare sistemi server fuori dal CED di Ateneo secondo le modalità previste dalle Linee guida, sollevando il Settore preposto e l'Ateneo da eventuali problemi di continuità dei servizi erogati.
4. È possibile ospitare, esclusivamente presso il CED di Ateneo, sistemi server in hosting e in housing secondo le modalità previste dalle Linee guida e regolamentate da opportune convenzioni.

Art. 20 Richiesta di servizi per progetti

1. Il Settore preposto ha il compito di gestire e monitorare tutti i servizi informatici che permettono il costante svolgimento delle attività istituzionali, di ricerca e di didattica. La richiesta di installazione e/o implementazione di ulteriori servizi e/o sistemi, specificatamente finalizzati allo svolgimento di progetti di ricerca/didattica o ulteriori servizi amministrativi, modifica necessariamente il Total Cost of Ownership (TCO) per l'impiego di risorse strumentali e umane per l'istallazione e la gestione dei
2. servizi nel tempo di vita del progetto. I servizi aggiuntivi dovranno essere valutati attraverso un progetto esecutivo secondo le modalità previste dalle Linee guida.

Art. 21 Delega applicativa

1. Così come previsto dalla vigente normativa in materia di protezione dei dati personali, è sempre possibile accedere a una o più applicazioni aziendali a nome di un diverso Responsabile o Incaricato, per un periodo di tempo obbligatoriamente predefinito. Tale funzionalità, conosciuta con il nome di delega applicativa, va considerata un evento eccezionale e dovrebbe essere concessa solo ed esclusivamente quando non vi siano altre opzioni percorribili.
2. Condizione necessaria affinché venga concessa una delega applicativa è l'invio, da parte del Direttore/Responsabile di Struttura, di una formale richiesta all'Ufficio Gestione Identità Digitali il quale, se non sussistono impedimenti di altra natura, applicherà la delega per il tempo strettamente necessario.

Parte V – Controlli e sanzioni

Art. 22 Controlli sull'osservanza del regolamento e sanzioni

1. L'Università degli Studi di Palermo, per garantire la funzionalità e la sicurezza del sistema informatico e nel rispetto di quanto previsto dall'art. 4, comma 2, dello Statuto dei lavoratori e dalla normativa di settore, si riserva di effettuare controlli c.d. 'indiretti' al fine accertare l'osservanza del presente Regolamento. Rispetto a tali controlli, lo stesso costituisce preventiva e completa informazione nei confronti degli utenti, interni ed esterni all'Ateneo.
2. Gli eventuali controlli, generali ed estesi, atti a individuare condotte non conformi al presente regolamento e alle Linee guida sui Servizi in rete, 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 regolamento, l'Ateneo 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'Ateneo 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.
6. L'utente è tenuto al rispetto del presente regolamento e delle Linee guida dei Servizi in rete.
7. L'inosservanza delle prescrizioni del presente Regolamento può comportare la restrizione o la revoca delle autorizzazioni ad accedere alla rete di Ateneo. Il personale del Settore preposto, valutata la gravità dell'eventuale illecito, provvede ad istruire la relativa pratica e a trasmetterla agli Organi competenti di Ateneo.

Art. 23 Norme finali

1. Per quanto non espressamente previsto dal presente Regolamento, si rinvia alle norme di Legge, allo Statuto e ai Regolamenti dell'Ateneo, alle norme di utilizzo della rete emanate dal Consortium GARR e ai provvedimenti dell'Autorità garante della protezione dei dati personali e alle circolari del Ministro della Funzione pubblica.

IL RETTORE
PROF. FABRIZIO MICARI

Firmato digitalmente da:Fabrizio Micari
Organizzazione:UNIVERSITA' DEGLI STUDI DI PALERMO/80023730825
Unita':RETTORE
Data:12/02/2020 16:16:45