UNIVERSITÀ DEGLI STUDI DI PALERMO

Versione 1.2 19/06/2024

LINEE GUIDA PER L'UTILIZZO DEI SERVIZI IN RETE

AREA SISTEMI INFORMATIVI DI ATENEO

SETTORE INFRASTRUTTURE E SERVIZI ICT

Responsabile: Carmelo Belfiore

Sommario

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

1. Finalità

Il presente documento, adottato in conformità alla policy di utilizzo della rete Garr, ispirato ai principi della Netiquette, secondo le indicazioni del Regolamento Generale sulla Protezione dei Dati e del Decreto Legislativo n. 196 del 23 giugno 2003, recante "Codice inmateria di protezione dei dati personali"; e secondo le indicazioni contenute nella deliberazione 1 marzo 2007 n. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e internet", ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio Internet e del servizio di posta elettronica da parte degli studenti e del personale dell'Università degli Studi di Palermo (nel seguito indicata semplicemente come UNIPA) e di tutti gli altri soggetti che a vario titolo utilizzano i servizi Internet e posta elettronica UNIPA.

2. Definizioni

- utente internet: persona autorizzata ad accedere al servizio internet;
- utente di posta elettronica: persona autorizzata ad accedere al servizio di posta
- elettronica;
- internet provider: chi fornisce a UNIPA il canale di accesso alla rete internet (GARR);
- postazione: personal computer collegato alla rete UNIPA tramite il quale l'utente accede ai
- servizi.
- Registro informatico dei software
- VPN (virtual private network) è una rete di comunicazione dati privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet
- Wi-Fi è una tecnologia che attraverso i relativi dispositivi consente a terminali di utenza di collegarsi tra loro attraverso una rete locale in modalità wireless (WLAN) basandosi sulle specifiche dello standard IEEE 802.11
- webmail (o "posta via web") e' un'applicazione web che permette di gestire la posta elettronica tramite un pannello accessibile direttamente dal proprio browser (Internet Explorer, Firefox, Safari e simili).
- Newsletter è un messaggio di posta elettronica inviato agli iscritti al servizio di un sito web per aggiornarli sulle novità di quest'ultimo

3. Il Settore Preposto

Il Settore preposto per il monitoraggio e la cura delle presenti Linee guida è il Settore servizi generali informatici di Ateneo.
Il Settore si avvale di quattro unità operative:

- Gestione e manutenzione portale di Ateneo e database;
- Sviluppo e manutenzione dei sistemi;
- Reti e sicurezza;
- Identity Management.

Esse collaborano alla corretta applicazione delle Linee guida.
Il Settore è responsabile del coordinamento degli Amministratori di Sistema (AdS) appositamente incaricati, con provvedimento formale, della gestione e/o della manutenzione di uno o più sistemi collegato/i alla Rete di Ateneo. Con riferimento al Provvedimento del 27 Novembre 2008 del Garante

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

della Privacy, sono da considerare, a tutti gli effetti, Amministratori di Sistema 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).

Il Settore è responsabile del mantenimento dei registri di sicurezza e degli inventari previsti dal Regolamento generale per la protezione dei dati personali 2016/679 (General Data Protection Regulation - GDPR).

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

4. Utilizzo Strumenti informatici

4.1 Utilizzo del Personal Computer

Il computer, di proprietà personale o acquistato sui fondi dell'Università di Palermo, che l'utente connette alla rete dell'Ateneo, diventa uno strumento di lavoro il cui utilizzo deve avvenire, nel rispetto dei principi di correttezza e diligenza, per perseguire finalità di tipo istituzionale e/o previste dalla legge.
Ogni utilizzo non conforme può causare disservizi, costi di manutenzione, minacce alla sicurezza delle risorse informative, danni a persone o al patrimonio universitario.
Ciascun Utente deve prestare la massima attenzione nell'utilizzo di supporti di memorizzazione esterna (*dispositivi usb, etc…)* e deve avvertire immediatamente l'AdS di riferimento nel caso in cui vengano rilevati virus o malfunzionamenti dei servizi di rete.
Le configurazioni standard del computer sono suggerite dal Settore preposto in base alle direttive di sicurezza e implementate dall'utente e/o dall'AdS di riferimento. Le configurazioni standard non devono mai essere modificate dall'utente autonomamente, anche nei casi in cui si posseggano i privilegi necessari. Eventuali modifiche devono essere comunicate sul registro informatico del software.
È opportuno che su tutti i PC connessi in rete, ogni utente, salvo eccezioni autorizzate, acceda con account che non abbia diritti di amministratore.
Ogni attività che richieda il privilegio di amministrazione (ad esempio installazione di software, stampanti, etc.), deve riferirsi all'AdS di riferimento. Il possesso e l'uso, da parte dell'utente, di account con diritti di amministratore manleva la responsabilità dell'AdS di riferimento e quindi del Settore preposto.
Per finalità di assistenza, manutenzione e aggiornamento e previo avviso all'utente, l'AdS può accedere da remoto, installando sulla postazione apposito software di controllo remoto, alla stazione di lavoro dello stesso, nel rispetto delle norme in materia di privacy.
È deprecata l'installazione di programmi diversi da quelli autorizzati; l'utente può altresì procedere all'istallazione, assumendosi la piena responsabilità per applicazioni pericolose per la sicurezza o che, in qualche modo, provochino disservizi, costi di manutenzione, danni a persone, al patrimonio universitario e/o alle risorse informative.
Durante la sessione di utilizzo del Personal Computer e al termine della stessa gli utenti non devono lasciare incustodito e accessibile il dispositivo; in particolare, il Personal Computer deve essere bloccato se si è in pausa pranzo e ogniqualvolta si abbandoni la propria postazione di lavoro per un consistente periodo di tempo; il Personal Computer deve essere spento al termine della sessione lavorativa (fine giornata lavorativa), salvo eccezioni autorizzate.

4.2 Utilizzo di postazioni di lavoro multiutente

L'accesso a sistemi multiutente è consentito attraverso la configurazione di più account locali o l'inserimento della postazione in un dominio di rete.
La configurazione della workstation è a carico dell'AdS di riferimento, che ne registra il nodo in rete e rilascia le credenziali agli utenti e cura la registrazione e conservazione dei log di accesso.
Le workstation possono rimanere accese durante le proprie sessioni di lavoro, anche concluse, e potranno essere raggiungibili da altri nodi della rete di Ateneo o dall'esterno in accordo con le specifiche al punto 5.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

4.3 Uso di sistemi personali

È consentito collegare alla rete di Ateneo sistemi di elaborazione che non sono di proprietà dell'Università (personal computer, portatili, palmari ecc.), purché vengano rispettate le prescrizioni indicate per i sistemi in uso presso l'Università, in particolar modo quelle relative ai sistemi di sicurezza. Sarà cura dell'AdS di riferimento registrare l'utente, rilasciare l'IP specifico per il PC personale e attuare tutte le strategie possibili (controllo dell'aggiornamento del sistema e dell'antivirus, presenza del firewall, scansione con tool di sicurezza e anti-malware) affinché il PC non sia né soggetto né oggetto di attacchi informatici, soprattutto se trattasi di notebook che spesso vengono connessi ad altre reti.

4.4 Responsabilità degli AdS

E' responsabilità degli AdS mantenere una rete integra, monitorata negli accessi e protetta dagli attacchi informatici, attraverso la corretta applicazione delle procedure su tutti gli strumenti informatici ad essa connessi.

Per tale motivo gli AdS incaricati devono avere pieno controllo dei sistemi a loro affidati o connessi alla rete a loro assegnata.

Nel caso in cui l'Utente desideri mantenere l'esclusivo controllo di strumenti informatici personali asserviti alle apparecchiature di ricerca e/o didattica di proprietà dell'Ateneo per casi specifici, manleva l'AdS con comunicazione ufficiale indirizzata al Settore preposto, diventando l'unico responsabile dei sistemi ad esso assegnati.

Se l'AdS si trova nell'impossibilità di svolgere i propri compiti istituzionali a causa del mancato accesso con credenziali di amministrazione, nel caso in cui l'utente non comunichi la manleva al Settore preposto, l'AdS può, in via cautelare, comunicare la manleva in autotutela. Sarà compito del Settore preposto comunicare all'utente la problematica e l'assegnazione d'ufficio della responsabilità sull'uso della rete e sulle procedure minime di sicurezza previste dall'Art.5

4.5 Strumenti e apparati di rete

Sulla rete di Ateneo e sulla sottorete di struttura possono essere connessi strumenti wired come stampanti, workstation, videocamere, sistemi di comunicazione etc.; sarà cura degli AdS di riferimento stabilire le configurazioni opportune e garantirne il corretto funzionamento.

Se non espressamente autorizzati dal Settore preposto, non è possibile connettere alla rete apparati di rete wireless, ad esempio access point, repeater, ecc…, o connettere altri apparati che possano compromettere o ridurre la sicurezza della rete e la funzionalità del servizio Wi-Fi.

Tutti gli apparati autorizzati connessi alla rete devono comunque essere certificati e devono essere inseriti nella topologia della rete da parte degli AdS, indicando le specifiche del servizio e le motivazioni dell'istallazione.

A meno di espressa autorizzazione da parte del Settore preposto (concessa solo per scopi istituzionali di didattica e/o ricerca), è vietata l'istallazione, su rete wired e wireless, di apparati di bridging, networkflow, packet inspection etc.

4.6 Protocolli specifici

E' possibile redigere specifici protocolli mirati a definire le modalità di accesso e uso per particolari strumenti e apparati informatici di interesse istituzionale e connessi alla rete di Ateneo.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

Tali protocolli devono essere redatti dai responsabili scientifici in accordo con gli AdS di riferimento e devono essere comunicati al Settore preposto che, dopo valutazione, redigerà le relative linee guida.

5. Modalità applicative delle misure minime di sicurezza

Le linee guida indicate nel presente documento fanno riferimento all'applicazione delle linee guida come da Circolare AGID 18 aprile 2017, n. 2/2017.

5.1 Le Famiglie di controlli

L'identificazione dei passi da adottare per definire i livelli di rischio informatico è estratta dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC "CIS Critical Security Controls for Effective Cyber Defense" nella versione 6.0 del 2015, e trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, in un equilibrato bilanciamento tra i costi di vario genere che l'implementazione di una misura di sicurezza richiede e i benefici che la stessa è in grado di offrire. L'elenco dei 20 controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi. In particolare, ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla propria.
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE ABSC 10 (CSC 10): COPIE DI SICUREZZA ABSC 13 (CSC 13): PROTEZIONE DEI DATI
Si comunica che i primi 5 controlli sono quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni. Poiché il CCSC è stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ai controlli delle prime 5 classi sono stati aggiunti quelli della CSC8, relativa alle difese contro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di perdita ed alterazione. Ciascun CSC è costituito da una famiglia di misure di dettaglio più fine, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realtà locale. E' stato introdotto un ulteriore terzo livello, nel quale la misura di secondo livello viene decomposta in misure elementari, ancora una volta implementabili in modo indipendente in funzione del livello applicativo minimo, standard o avanzato. L'implementazione di misure a livello applicativo standard o avanzato per la stessa famiglia di misure costituisce un livello di sicurezza maggiore rispetto al livello applicativo minimo.
E' complito di tutti gli AdS applicare tutti i suddetti controlli relative alle 8 famigli elencate registrando su appositi registri elettronici le modalità e l'avvenuta applicazione delle misure per ogni sottoclasse definita e applicabile al relativo servizio, sistema informatico e/o apparato.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

5.2 Risorse on-line

Le risorse e gli aggiornamenti normativi relativi all'argomento, pubblicati on-line sui siti dell'AgID e Cert PA, costituiscono parte integrante delle presenti Linee Guida.
Sarà compito del Settore preposto dare massima diffusione in merito alle nuove normative, procedure e disposizioni a tutti gli AdS attraverso il sito istituzionale, con mezzi di comunicazione asincrona.

6. Identity Management – Specifiche tecniche e modello operativo

6.1 Identity Management

L'Ateneo adotta un sistema di Identity Management (IM) che consente di gestire l'intero ciclo di vita delle identità utente e delle credenziali associate. Il sistema è stato configurato per la sincronizzazione delle identità, la gestione centralizzata di certificati e password e il provisioning degli utenti in tutti i sistemi eterogenei presenti in rete. Esso acquisisce le identità dalle fonti autorizzative e popola, in funzione dei ruoli assegnati e dei permessi applicativi e temporali dell'identità stessa, i sistemi di "directory" di Ateneo quali LDAP, RADIUS, Microsoft Active Directory (alla base dei servizi di rete e applicativi), consentendo al Settore IT di definire e automatizzare i processi di gestione delle identità, dalla creazione al ritiro.
Il sistema estende queste funzionalità di IM aggiungendo il controllo degli accessi in base al ruolo assegnato. Nel sistema sono stati definiti i 'ruoli utente' e le autorizzazioni per controllare l'accesso ai dati e alle applicazioni sensibili. Il sistema di Identity Management esegue il mapping di queste funzioni e verifica che le definizioni dei ruoli e i diritti associati siano applicati correttamente agli utenti.

6.2 Controllo di accesso in base ai ruoli Role-based access control (RBAC)

Il controllo degli accessi in base al ruolo consente di implementare questi criteri in modo automatico. E' possibile quindi specificare e strutturare i ruoli nell'organizzazione, eseguire il mapping di utenti a determinati ruoli ed eseguire il mapping delle autorizzazioni appropriate a ogni ruolo. Questa struttura, detta modello a ruoli, contiene e connette tra loro cinque tipi di oggetti:

1. Unità organizzative
2. Users
3. Ruoli
4. Autorizzazioni
5. Applicazioni

L'unità organizzativa è alla base della gerarchizzazione degli utenti nel sistema di modello a ruoli. Ogni utente deve appartenere ad almeno un'unità organizzativa. Quando un utente viene rimosso dall'ultima unità organizzativa, il record dei dati dell'utente viene eliminato dal database.
Nel modello a ruoli è possibile consentire l'assegnazione di ruoli a utenti esterni (ad esempio, i dipendenti di un fornitore esterno) che quindi potranno accedere alle risorse IT senza essere aggiunti al database dei dipendenti, ma a specifiche altre fonti di dati.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

6.3 Gestione del sistema Identity Management

La gestione della definizione dei ruoli e dei relativi permessi e autorizzazioni, sulla base dei servizi cui si intende avere accesso, è affidata al sistema A3, implementato a supporto del servizio di Identity.
I ruoli attivi vengono raggruppati e definiti sulla base di ruoli e funzioni stabiliti o raccolti nelle basi autorizzative di Ateneo, raccolte dal data warehouse UNIDB, sia per quanto riguarda il personale interno che gli studenti.
Su tale base, per ogni ruolo vengono definite le tipologie (amministrativo, didattico, scientifico), i permessi per gruppo di servizi e/o applicazioni a livello di accesso, nonché il periodo temporale di autorizzazione per quel gruppo di permessi.
Tutti i ruoli amministrativi relativi al personale strutturato decadono una volta cessato il rapporto giuridico intercorso con l'Ateneo; per esigenze istituzionali e/o di servizio, è possibile estendere il periodo di validità dei ruoli didattici e scientifici rispetto al ruolo amministrativo. In questi casi sarà cura dell'applicativo o del servizio garantire la corretta profilazione dell'utente.
Tutti i ruoli amministrativi relativi agli studenti sono definiti e aggiornati in base alla normativa vigente di settore e alle relative circolari ministeriali. E' necessario garantire quanto più possibile la continuità e la fruibilità dei servizi a loro dedicati.
La mappatura dei ruoli, dei servizi e delle autorizzazioni per servizio con le relative scadenze, dovrà essere comunicato ad ogni utente ed al proprio responsabile attraverso un processo automatico di segnalazione.
Ogni servizio quindi, esposto al sistema di IM, deve fornire i ruoli autorizzati e il periodo temporale in cui il servizio è attivo per il ruolo, il possibile periodo di retention dopo il quale il servizio viene sospeso e il periodo di pending delete dopo il quale il servizio viene cessato.
Il raggruppamento tabellare di tutti i servizi e dei relativi tempi di estensione del ruolo rispetto al periodo di fine rapporto con l'Ateneo deve essere pubblicato e aggiornato sul sito istituzionale e/o comunicato per mezzo della carta dei servizi.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

7. Servizi in Rete

7.1 Generalità

L'uso della rete di Ateneo è finalizzato a scopi didattici, di ricerca e allo svolgimento delle attività istituzionali dell'Università degli Studi di Palermo.
Per garantire quindi l'uso, l'integrità della rete aziendale deve essere scrupolosamente protetta da appositi dispositivi di sicurezza informatica (firewall, idp, antivirus, ecc.).
Per tali ragioni di sicurezza, non possono essere collegate alla rete universitaria apparecchiature senza il coinvolgimento degli AdS di riferimento della Struttura o, in assenza di questi, del personale afferente al Settore preposto.
Per tali motivi l'utente **non deve**:

1. utilizzare sistemi operativi obsoleti e/o inaffidabili collegati alla rete;
2. utilizzare strumenti *software* e/o *hardware* atti a perpetrare illeciti informatici;
3. cedere a persone non autorizzate e lasciare incustodita la propria postazione, una volta superata la fase dell'autenticazione e/o dell'applicazione a cui si è avuto accesso, fornendo il servizio di connettività di rete a Utenti non autorizzati all'accesso alla rete;
4. utilizzare applicativi o servirsi di risorse o tunnel che consentono di restare anonimi durante l'uso della rete;
5. installare applicativi o servizi che permettono di scavalcare gli obblighi contrattualmente assunti dall'Università e di non rispettare la normativa di riferimento in materia di copyright, licenze d'uso di software e connettività di rete compiendo azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore;
6. 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;
7. distruggere, danneggiare, intercettare o accedere senza autorizzazione a risorse in rete 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.

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.
Inoltre, sulla base del monitoraggio dei sistemi di Ateneo di intrusion e prevention detect e/o sulla base delle comunicazioni del GARR, l'accesso alla rete d'Ateneo può essere revocato a ogni utente strutturato fino alla risoluzione dell'eventuale problema di sicurezza sui propri apparati.

7.2 Mappatura IP e porte standard

Ad ogni sistema attivo sulla rete di Ateneo deve avere associato un indirizzo IP, rilasciato in modalità dinamica da un servizio DHCP autorizzato o in modalità statica dall'AdS della Struttura di riferimento (Facoltà, Dipartimento, Segreteria Studenti, Uffici amministrativi, aule didattiche, …). L'AdS deve registrare sull'apposito sistema di registro informatico l'associazione tra l'indirizzo IP rilasciato e la persona fisica responsabile che lo sta utilizzando per il proprio sistema. In mancanza di tale figura, l'associazione dovrà essere effettuata dal personale afferente al Settore preposto a seguito di una richiesta formulata dall'utente o dal responsabile.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

Ogni appropriazione indebita dell'indirizzo IP e conseguente abuso nello stato di sostituzione di persona, può dare luogo alla revoca di accesso ai servizi di rete e alla comunicazione, da parte del personale del Settore preposto, agli Organi competenti per la verifica di eventuali responsabilità disciplinari.
Ogni utente può essere intestatario di diversi indirizzi IP ed è propria la responsabilità del corretto uso dei sistemi associati. L'utente è tenuto a comunicare nel minor tempo possibile il deprovisioning dell'IP dai sistemi obsoleti o non più funzionanti in rete, sia per consentire il rilascio dell'IP ad altri utenti, sia per evitare la propria responsabilità su un possibile abuso dell'indirizzo.
E' responsabilità dall'AdS della Struttura di riferimento monitorare gli IP assegnati ai sistemi attivi acquistati dalla struttura o in carico alla stessa.
E' responsabilità del personale del Settore preposto monitorare gli IP assegnati ai sistemi attivi acquistati per tutto l'Ateneo o in carico alla stessa e istallati presso le strutture di ateneo.
E' compito del Settore preposto fornire agli AdS gli strumenti e l'opportuno know-how al fine di consentire il rilevamento degli indirizzi IP che subiscono cambio di MAC o che vengono bannati per le comunicazioni di sicurezza.
Tutti i sistemi devono essere abilitati in rete all'utilizzo delle porte standard secondo una profilatura che viene stilata periodicamente e pubblicata dal Settore preposto in virtù delle analisi di sicurezza volte a minimizzare il rischio di attacchi informatici.
Ove possibile, a cura dell'AdS, occorre configurare i sistemi in rete chiudendo le porte non standard, attraverso la disattivazione dei servizi sui sistemi e/o installazione e configurazione di applicativi firewall che consentono di rispettare la suddetta profilatura.
Al fine di rispettare le politiche del GARR ed essere a norma con le misure minime di sicurezza, non è consentito l'apertura di specifiche porte non standard sui sistemi firewall di frontiera di Ateneo; specifiche necessità di porte non standard comporteranno l'apertura di tutte le porte per l'IP specifico attribuendo all'utente o all'AdS, l'onere e la responsabilità di mettere in sicurezza tale sistema attraverso l'opportuna configurazione del firewall locale.
La tipologia di tali richieste di sistemi con IP all-to-all utilizzate dovranno essere registrate sul sistema di registro informatico; in ogni caso la piena responsabilità rimane in capo all'utente e all'AdS che ha il compito di monitorare il corretto uso della connessione e dei servizi applicativi istallati.

7.3 La connessione di aule e laboratori informatici

Le aule e i laboratori informatici sono sotto la diretta responsabilità degli AdS di riferimento e di norma sono collegati alla rete di Ateneo in modalità wired con rilascio IP dinamico tramite DHCP locale o IP assegnato staticamente.
Al fine di minimizzare il rischio informatico, è opportuno che aule e laboratori siano associati a reti isolate attraverso l'utilizzo di specifiche VLAN e opportuni profili delle politiche di routing sui gateway di uscita. A tal fine, su autorizzazione, è possibile utilizzare sottoreti private non ruotabili, con conseguente implementazione da parte degli AdS di riferimento dei servizi di firewall, NAT, Proxy e SysLog necessari ad ottemperare le disposizioni di legge e del Garante della Privacy in modo da garantire il controllo e il monitoraggio del traffico. In tal caso la sottorete deve essere connessa fisicamente ad un apparato attivo management e il Settore preposto monitorerà il traffico sul relativo gateway, mentre sarà responsabilità degli AdS mantenere il registro dei log e l'identificazione degli accessi alle postazioni di lavoro personali e multiutenti.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

8. Servizi di rete

I servizi di rete possono essere fruiti da tutti gli utenti profilati dal sistema centralizzato di identity management o profilati direttamente dal servizio di rete in accordo all'art.7

L'accesso ai servizi di rete per utenti afferenti ad Enti strumentali/convenzionati/consorziati con UNIPA deve essere regolamentato in apposite convenzioni con gli stessi definendo le responsabilità per un uso non corretto che possa compromettere le normali attività istituzionali. Il riconoscimento dell'utente rimane a cura dell'Ente strumentale/convenzionato/consorziato.

L'elenco dei servizi di rete è contenuto all'interno delle presenti Linee Guida che descrivono anche le caratteristiche proprie di ogni servizio, le eventuali modalità di provisioning e deprovisioning delle utenze e il periodo temporale certo di autorizzazione alla risorsa.

Tutti i servizi che prevedono un accounting operativo o di servizio devono essere elencati nel sistema di "registro elettronico dei servizi" insieme alle operazioni di autorizzazione e di eventuale proroga all'utilizzo.

L'accesso ad ogni servizio dovrà essere sospeso in automatico alla data di fine del periodo temporale di autorizzazione. Il servizio dovrà essere cessato, dopo la data istituzionale di fine rapporto con l'Ateneo, se vengono superati i 6 mesi di inattività dall'ultimo uso.

8.1 VPN

L'Università degli Studi di Palermo mette a disposizione tale servizio per un gruppo / ruolo di utenti che ha la necessità di collegare il proprio pc al di fuori del perimetro della rete di Ateneo, utilizzando la rete pubblica internet, per accedere in sicurezza ad applicativi software o web Application dell'Ateneo e svolgere le normali applicazioni di ufficio.

Per tali ragioni il servizio è dedicato principalmente a proteggere protocolli di rete no web based come rdp, ssd, ftp e aumentare la sicurezza di accesso a siti web di backoffice su protocollo SSL. Il servizio è di esclusiva implementazione del Settore preposto e, per ragioni di sicurezza, non sono permessi creazioni di ulteriori e personali servizi VPN all'interno della rete di Ateneo; eventuali necessità di connessioni VPN per istallazioni e/o manutenzioni di apparati devono essere comunicate all'AdS locale che valuterà le opportune configurazioni con il Settore preposto, il quale valuterà il rilascio della relativa autorizzazione.

Ai fini della valutazione dei rischi, tutte le configurazioni delle reti VPN devono essere registrate; per ogni servizio VPN devono essere descritti i modelli di flusso dati, che ne definiscono i punti sorgente/destinatario con le relative interfacce di gateway, il ruolo degli utenti utilizzatori e il periodo temporale di attività del servizio.

Mentre la connessione VPN è attiva, tutti gli accessi esterni alla rete di Ateneo devono passare per lo stesso firewall, come se l'utente fosse fisicamente connesso all'interno della rete.

Il servizio VPN viene autorizzato/deautorizzato per singolo utente e per ruolo; non si prevede retention time, nè periodo di pending delete. La disattivazione avverrà alla scadenza del periodo di autorizzazione e/o del ruolo.

Gli AdS e/o il Settore preposto sono tenuti al monitoraggio e all'audit degli accessi degli utenti attraverso il servizio VPN, che necessariamente deve essere implementato sempre secondo le specifiche tecniche di accesso centralizzato previste dal sistema di Identity Manager.

Un utente autenticato può essere provvisto di privilegi particolari per accedere a risorse che generalmente non sono accessibili alla generalità degli utenti.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

8.2 Wi-Fi

Il servizio, fruibile attraverso le proprie credenziali di Ateneo e attraverso EDUROAM, è disponibile in federazione anche ad utenti che provengono da altri Atenei e/o Enti di ricerca.
Ai fini della valutazione dei rischi e del rispetto delle norme sulla privacy, è necessario isolare la navigazione in funzione dei destinatari del servizio. In questo modo, è possibile ridurre il perimetro di attacco definendo opportune policy di accessibilità relative al personale strutturato, al personale studente, al personale riconosciuto tramite federazione nonché al personale ospite presente all'interno del Campus in occasione di convegni, meeting, manifestazioni, inviti o altro.
Il servizio di rete WI-FI è fornito mediante l'utilizzo di frequenze in banda condivisa, la fruizione quindi del servizio e la sua qualità non sono garantite.
L'Ateneo non è responsabile verso l'utente e/o verso terzi per i danni diretti o indiretti, derivanti da sospensioni o interruzioni del servizio.
L'utilizzo è comunque soggetto al rispetto delle norme vigenti, delle condizioni contenute nel presente disciplinare e delle regole tecniche, che si intendono implicitamente accettate con il primo utilizzo del servizio stesso.
Su opportuno registro informatico dovranno essere esplicitamente indicati, per ogni SSD di rete WI-FI disponibile e/o implementata, i ruoli ai quali si permette l'accesso, i modelli di accesso e istradamento e i tempi di utilizzo del servizio.
Il servizio WI-FI viene autorizzato/deautorizzato per singolo utente e per ruolo; non si prevede redemption time, nè periodo di pending delete. La disattivazione avverrà alla scadenza del periodo di autorizzazione e/o del ruolo.
La registrazione di utenti ospiti e la creazione di un account temporaneo per convegni, meeting e manifestazioni e eventi simili sono a cura degli AdS locali e/o del Settore preposto e dovrà avvenire manualmente o attraverso un sistema automatico, con garanzia dell'individuazione dell'utente.
Ai fini della sicurezza dell'intera rete di Ateneo, è vietato istallare apparati Access Point non autorizzati e connetterli alla rete wired, e/o creare sotto reti wireless 2,5/5 GHz per tunneling point- to-point o point-to-multipoint wireless, secondo quanto definito nell'art.3.

8.3 Servizi web

Tutti i servizi web devono essere implementati nel rispetto dei principi di sicurezza del dato, in aderenza al modello privacy-by-default e privacy-by-design. La divulgazione e/o pubblicazione dei dati deve avvenire nel rispetto delle norme sulla privacy.
In particolare, l'interfaccia web deve comunicare attraverso protocollo SSL, non deve permettere crosscript ed escalation protocol, deve essere implementata, possibilmente, su un server in zona DMZ, oppure attraverso l'opportuna configurazione di VLAN o di zone di servizi gestiti da firewall.
L'applicativo web deve comunicare in modo esclusivo con la relativa base dati su protocollo protetto o controllato e non deve permettere la consultazione o l'accesso diretto al dato.
Tutti i servizi web che richiedono l'autenticazione e accesso da parte degli utenti devono essere sviluppati secondo lo standard aperto Security Assertion Markup Language (SAML), implementando il servizio Shibboleth in accordo con l'Art. 6.
In accordo con le misure minime di sicurezza, tutti i servizi web devono essere registrati su registro informatico. In questo devono essere registrate tutte le informazioni delle specifiche tecniche e delle relative dipendenze funzionali da altri servizi.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

9. Sistemi di comunicazione Asincrona

9.1 E-mail istituzionale

Il servizio e-mail istituzionale personale è attivo giuridicamente sul dominio unipa.it e mette a disposizione una casella e-mail per le utenze fisiche censite e abilitate dal sistema di Identità digitale di Ateneo in base al ruolo ricoperto.
In particolare, la casella e-mail istituzionale viene abilitata a tutto il personale strutturato dell'Ateneo, ai dottorandi, specializzandi e assegnisti di ricerca, con carriera giuridicamente attiva.
Poiché l'invio di posta elettronica dalle caselle istituzionali può ingenerare nel destinatario del messaggio la convinzione di una relazione stretta di appartenenza specifica del mittente all'Ente UNIPA, l'assegnazione del servizio di e-mail istituzionale personale è esclusa per i ruoli professionali e/o di consulenza con contratti attivi non subordinati e/o con attività limitata nel tempo.
Il servizio e-mail istituzionale di struttura è attivo, giuridicamente, su domini di terzo livello quali uffici.unipa.it, dipartimenti.unipa.it, sba.unipa.it, etc. con possibile alias sul dominio unipa.it.
È possibile assegnare una o più caselle per ogni ufficio/struttura giuridica amministrativa dell'Ateneo, secondo le esigenze manifestate, al Settore preposto, dagli uffici e dalle strutture stesse.
Il personale docente in quiescenza, ai sensi dell'Art. 7 comma 5 del "Regolamento sull'utilizzo della Rete di Ateneo e dei Servizi Internet", potrà utilizzare il servizio e-mail istituzionale per ulteriori 12 mesi dalla scadenza del contratto. Successivamente a tale periodo sarà attivata una mail su dominio di terzo livello "@people.unipa.it", da rinnovare ogni 24 mesi previa autorizzazione del Rettore o di un Direttore di Dipartimento. Il docente in quiescenza potrà continuare a ricevere e-mail anche su alias del dominio "@unipa.it", ma potrà inviare e-mail solo con dominio di terzo livello "@people.unipa.it".
Analogamente, anche per il personale TAB in quiescenza, previa autorizzazione del Direttore Generale, per specifiche esigenze, si potrà attivare su dominio di terzo livello l'account di posta elettronica per 24 mesi, rinnovabili.
Non è possibile l'attivazione di caselle e-mail istituzionali di struttura per uffici e/o strutture nelle quali l'Ateneo non sia giuridicamente coinvolto con partecipazione attiva o tramite convenzione fra Enti.
Ogni casella e-mail istituzionale di struttura è assegnata ad un unico responsabile (persona fisica), al quale vengono consegnate, dal sistema di posta, le relative credenziali di accesso attraverso la propria e-mail istituzionale personale e le specifiche per la configurazione di accesso.
In caso di accesso multiutente, fatta salva la deroga applicativa per limitati e certificati periodi temporali, è necessario configurare l'e-mail istituzionale di struttura su un sistema di gestione (ad es. ticket OTRS) che permette a più utenti di accedere, con le proprie credenziali, a una web application, visionare la posta in arrivo e inviare messaggi in nome e per conto dell'ufficio sottoscrivendo, in modo automatico, l'identità del mittente.

9.1.1 Gestione e utilizzo del sistema e-mail

L'erogazione del servizio di posta elettronica, può avvenire anche utilizzando anche server di Provider esterni, certificati secondo le disposizioni dell'AgID e del Garante della Privacy, individuati mediante gare ad evidenza pubblica e/o convenzioni. Su questi, ogni utente avrà a disposizione una casella di posta elettronica, oltre alla possibilità di utilizzare tutti i servizi aggiuntivi forniti nell'ambito della convenzione stipulata tra l'Università ed il Provider. La pagina di Login alla casella di posta è ospitata sul sito istituzionale dell'Ateneo. Il servizio è consentito anche attraverso l'utilizzo di programmi di posta personali ed apparati mobili che rispettino i protocolli standard di comunicazione sulla rete.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

Gli utenti del servizio di posta elettronica sono tenuti ad adottare tutte le misure idonee per non interferire con il corretto funzionamento della stessa e per assicurare agli altri utenti il godimento del medesimo servizio.
In ottemperanza alle norme vigenti, i sistemi informatici a supporto del servizio e-mail devono garantire la riservatezza, l'immodificabilità e la sicurezza del contenuto dei messaggi, fatte salve le normali operazioni di intercettazione, da parte di appositi filtri automatici, di virus o spam contenuti nei messaggi stessi.
I server di posta elettronica sono infatti dotati di strumenti di protezione logica costantemente aggiornati ed atti a contenere i rischi derivanti da possibili incidenti informatici. Resta evidentemente in capo ad ogni singolo utente la responsabilità di un atteggiamento consapevole nei confronti di tali insidie.
Gli utilizzatori del servizio di posta elettronica devono segnalare al settore preposto e-mail aventi mittente, oggetto o allegati incerti o sospetti, successivamente è consigliabile cancellare il messaggio di posta.
L'Ateneo utilizza opportuni sistemi antispam e antivirus, ossia dei sistemi che consentono di bloccare la propagazione di spam e virus, ed eventuali azioni illecite, per quanto possibile. I messaggi "taggati" come [SPAM] sono messaggi identificati dal sistema come messaggi indesiderati, per cui si invita a verificarne la provenienza e valutare la loro cancellazione.
È fatto divieto agli utenti di utilizzare lo strumento della posta elettronica per inviare, trasmettere o comunque divulgare a terzi non autorizzati informazioni riservate dell'ufficio e/o dell'Ateneo.
La casella di posta istituzionale personale o di struttura, assegnata dall'Università all'utente, è sempre uno strumento di lavoro e, come tale, deve essere utilizzata per perseguire fini istituzionali. Gli operatori assegnatari delle caselle di posta elettronica sono responsabili quindi del corretto utilizzo delle stesse. Non è consentito fornire a soggetti terzi non autorizzati l'accesso al servizio di posta elettronica istituzionale personale e tantomeno di struttura.
In caso di assenza dal servizio dell'utente per brevi periodi, è a disposizione apposita funzionalità di sistema, che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando, eventualmente, altre modalità di contatto con la struttura.
L'accesso alla propria e-mail istituzionale personale non può essere delegato, in quanto le credenziali di accesso d'Ateneo sono uniche e valgono anche per tutti gli altri servizi che utilizzano il sistema di Identity Management; per tale motivo è determinante veicolare i messaggi istituzionali di ufficio alle caselle email di struttura, in modo che l'accesso possa essere delegato o i messaggi possono essere veicolati tramite il sistema di gestione multiutente (es. ticket OTRS).
Al fine di limitare il perimetro di attacco informatico e minimizzarne il rischio, la gestione della posta elettronica deve essere fatta, di norma, utilizzando la webmail; sono, tuttavia, consentiti i client IMAP, POP e SMTP su secure layer esclusivamente dalla rete di Ateneo o da altre reti esterne tramite accesso VPN.
È buona regola la periodica 'pulizia' della casella di posta, con la cancellazione di e-mail obsolete ed inutili e la contestuale archiviazione dei messaggi meno recenti, spostandoli dalla casella di posta in arrivo.
Il sistema email è un servizio di comunicazione asincrona e non un sistema per la condivisione dei file, pertanto eventuali allegati di grande dimensione o in numero elevato devono essere trasmessi in formato compresso (zip, rar). Per comunicazioni quindi tra gli uffici dell'Ateneo è bene limitare

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

l'uso della posta alla sola comunicazione e utilizzare, per il trasferimento dei file, i servizi di condivisione dei file, disponibili anche tramite la webmail.
Il personale del Settore preposto non può esercitare visura, controllo, censura, modifica, cancellazione dei messaggi di posta elettronica istituzionale personale ricevuti e inviati dagli Utenti; 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 o ad un ordine giudiziario.
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, verranno memorizzati con retention time di 365 giorni, e archiviati secondo le profilature tecniche del servizio di backup.
Al fine di garantire un servizio efficiente, è buona norma osservare correttamente le specifiche del sistema email: mettere in A: solo gli indirizzi a cui la missiva è direttamente destinata, mettere in copia conoscenza (CC:) solo i destinatari ufficiali di cui non ci si aspetta risposta; e, per limitare possibili loop reply quando ho un numero elevato di destinatari da raggiungere, mettere questi indirizzi in copia conoscenza nascosta (CCn:).
Per non abbassare l'indice di reputazione del dominio unipa.it nei confronti dei domini destinatari, attualmente non è possibile ricevere o spedire messaggi di posta con allegati superiori ai 50 MB, non è possibile inviare in contemporanea lo stesso messaggio a più di 20 destinatari esterni e a più di 100 destinatari interni.
Laddove le Strutture avessero la necessità di inviare comunicazioni ad una pluralità di destinatari, deve essere usato il servizio di newsletter o il servizio *mailing list.*
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 all'ufficio indicato su apposita autorizzazione del Direttore Generale.
Gli indirizzi di posta elettronica istituzionali personali vengono mantenuti attivi, dal sistema di Identity manager, fino a 180 giorni dopo la data di fine del rapporto giuridico intercorso con l'Ateneo, trascorsi i quali la casella viene sospesa e non può né ricevere né inviare e-mail.
Successivamente alla data di fine del rapporto giuridico intercorso con l'Ateneo, l'inattività di accesso alla casella e-mail personale per 180 giorni consecutivi (pendig delete) ne decreta la sospensione d'ufficio e la cancellazione di tutti i messaggi ivi contenuti.
L'indirizzo e-mail istituzionale personale è legato strettamente all'utenza e non può più essere usato per altri omonimi, al fine di evitare sostituzione di identità. Per tale ragione, la casella e-mail rimane sospesa ma disponibile, in caso lo stesso utente riapra il ruolo, anche a distanza di tempo, con un nuovo contratto con l'Ateneo.
L'Ateneo si riserva il diritto di sospendere o cessare d'ufficio l'utilizzo della posta elettronica personale o di struttura all'utente allorché venga meno la condizione di utente autorizzato dello stesso per motivi gravi e accertati.

9.2 E-mail studenti

L'Ateneo fornisce il servizio di posta elettronica agli studenti, purchè abbiano una carriera attiva, per le comunicazioni di tipo istituzionale. Laddove lo studente abbia terminato il rapporto con l'Ateneo e non desideri più ricevere comunicazioni istituzionali inerenti al suo percorso didattico o formativo,

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

può espressamente richiedere la cancellazione degli account e dalle eventuali liste. In quest'ultimo caso, poiché l'indirizzo e-mail istituzionale è legato strettamente all'utenza, per evitare sostituzione di identità, l'account viene sospeso; la casella e-mail rimane disponibile in caso di future attivazioni. L'Ateneo si riserva, in ogni caso, la possibilità di sospendere, cessare o trasformare il servizio secondo le esigenze didattiche e/o amministrative, dandone comunicazione agli interessati.
Il servizio e-mail studenti è attivo giuridicamente sul dominio community.unipa.it su piattaforma Google e sul dominio you.unipa.it su piattaforma Office365.
Il sistema di IM rilascia le autorizzazioni di accesso alle piattaforme in cui lo studente può fruire anche di ulteriori servizi messi a disposizione dai relativi Provider.
L'Ateneo non fornisce supporto né garantisce la funzionalità dei servizi interamente gestiti dai fornitori esterni. Tuttavia, è compito del Settore preposto monitorare i servizi e garantire l'interoperabilità con il servizio di Identity Management.
Gli studenti sono tenuti ad utilizzare gli indirizzi di posta elettronica forniti dall'Ateneo per qualsiasi comunicazione istituzionale.
Il rilascio della casella avviene in modo automatico una volta profilato l'utente e abilitato il ruolo; le caselle devono essere abilitate con un primo accesso in cui i provider non devono richiedere informazioni personali.
Eventuali disservizi potranno essere comunicati al Settore preposto attraverso gli opportuni canali di comunicazione. L'Ateneo non è responsabile di eventuali disservizi prodotti non per propria causa, ma ha l'obbligo di vigilare sul corretto funzionamento del servizio di posta studenti, perché, attraverso questo, possono essere veicolate informazioni istituzionali riguardanti esami e/o lezioni.
Al fine di garantire la continuità del servizio, anche per l'e-mail studenti valgono le indicazioni sull'utente e sull'uso della posta elettronica espresse al punto 7.1.

9.3 Webmail

L'Ateneo rilascia il servizio webmail per il dominio istituzionale all'url *webmail.unipa.it* e, per l'accesso alle caselle di struttura, all'url *webmailstrutture.unipa.it.*
La webmail deve soddisfare le specifiche previste dall'art.5 e deve essere conforme alle misure di sicurezza, nel garantire la corretta esposizione e pubblicazione dei dati e la loro riservatezza.

9.4 Newsletter

È possibile creare in Ateneo un servizio dedicato di newsletter con i seguenti requisiti:

1. registrazione volontaria con controllo indirizzo e-mail da parte di tutti gli utenti del web;
2. compilazione di liste e-mail multiple a cui il sistema invia le informazioni sull'argomento;
3. sottoscrizione degli argomenti da parte dei relativi uffici dell'Ateneo o dei vari gruppi di ricerca;
4. gestione e compilazione dei bollettini comunicativi per argomenti da parte dei relativi uffici dell'Ateneo o dei vari gruppi di ricerca;
5. gestione degli inviti a sottoscrivere la newsletter e i relativi argomenti trattati.

L'invio di messaggi attraverso le newsletter deve rispettare la normativa vigente in termini di uso di reti telematiche, ed in particolare quanto indicato nell'art.18.
Essendo un servizio web, il servizio di newsletter deve soddisfare le specifiche previste dal punto 6.3 delle presenti Linee guida, dev'essere conformarsi a quanto previsto dalla vigente normativa in

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

materia di sicurezza e protezione dei dati, nonché della restante normativa di settore, nel garantire la corretta esposizione, pubblicazione/diffusione dei dati e la loro riservatezza.

9.5 Mail List

L'Ateneo di Palermo intende favorire la diffusione, tra il proprio personale, di informazioni riguardanti la vita dell'Ateneo tramite l'uso della Mailing List. Tale servizio è esclusivamente finalizzato all'invio di informazioni di tipo Istituzionale che non siano più efficacemente veicolabili attraverso altri canali, limitando il più possibile il rischio di usi impropri e non legittimi della Mailing List quali, ad esempio, la diffusione di informazioni false, offensive o lesive dell'immagine dell'Ateneo e rendendo chiaramente identificabile la struttura e il responsabile dell'invio di ciascun messaggio che utilizzi la Mailing List.
Il servizio mail list è reso disponibile dall'Ateneo alle strutture e/o uffici, per attività istituzionali e di servizio, al fine di inviare massivamente una stessa comunicazione via e-mail tra più destinatari coinvolti nella stessa lista.
Le Mailing List, in ogni caso, non possono essere utilizzate come sede di discussioni, per le quali altri strumenti (ad esempio blog o chat) sono più adeguati, o per la promozione di prodotti, servizi, iniziative o eventi non offerti dall'Ateneo e che non contribuiscono direttamente al raggiungimento dei suoi fini istituzionali.
In Ateneo possono essere attivate esclusivamente liste moderate, istituzionali, di struttura e di servizio.
La creazione di liste di distribuzione è a cura del personale del Settore preposto. L'elenco degli indirizzi e-mail può essere associato alla lista di distribuzione attraverso sistemi di estrazione automatica in base a criteri specifici, oppure manualmente attraverso la produzione di specifici file o, infine, tramite volontaria sottoscrizione alla lista esistente.
L'invio di messaggi attraverso le Mailing List deve rispettare la normativa vigente in termini di uso di reti telematiche ed in particolare:

- L. 23 dicembre 1993 n. 547 - Modificazioni ed integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica;
- D. Lgs. 196/03 (Codice in materia di protezione dei dati personali) così come modificato dal D. Lgs. 101/2018;
- D. Lgs. 6 settembre 2005 (Codice del Consumo);
- D. Lgs. 70/2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici della società dell'informazione, in particolare il commercio elettronico, nel mercato interno);
- D.P.R. 28 dicembre 2000 n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), così come modificato dal D. Lgs. 5 marzo 2005 n. 82 (Codice dell'amministrazione digitale);
- L. 22 Aprile 1941, n. 633 in materia di disposizioni sul diritto di autore, e successive modifiche.
- Codice di Comportamento dell'Università degli Studi di Palermo.

Tutte le mail-list create in Ateneo devono essere moderate da un responsabile, che ha l'onere di inviare l'informazione alla lista o di concedere la veicolazione dei messaggi alla lista. L'abilitazione ad accedere al servizio come moderatore verrà concessa previa sottoscrizione dell'impegno ad utilizzare tali servizi nei limiti e secondo le norme definiti dalle presenti Linee guida. Tale impegno implicherà l'esplicita accettazione delle regole d'uso del servizio, in particolare in termini di impegno

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

ad utilizzarlo esclusivamente per la distribuzione di informazioni di tipo istituzionale e legate al proprio ruolo o per gli scopi autorizzati.
L'eventuale uso scorretto dei servizi da parte di dipendenti dell'Ateneo verrà segnalato per gli opportuni provvedimenti. Gli autori dei messaggi inviati attraverso il servizio sono sempre responsabili in via esclusiva, civilmente e penalmente, per i contenuti veicolati.
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 devono essere inclusi nel corpo del messaggio.

9.5.1 Liste istituzionali

Per lista istituzionale si intende un indirizzo di posta elettronica al quale viene associato un elenco di indirizzi di e-mail istituzionali personali (unipa.it). Tale lista è moderata da uno o più responsabili ed è finalizzata all'esercizio delle funzioni istituzionali, per cui possono essere veicolate esclusivamente comunicazioni istituzionali volte all'espletamento delle funzioni proprie dell'Ateneo; non è, pertanto, prevista la cancellazione dalla lista e la possibilità di inviare risposte o repliche a tutta la lista da parte dei singoli utenti.
Le liste istituzionali, che possono riguardare sia argomenti di interesse generale che specifico, veicolano le comunicazioni inviate dai soggetti istituzionali di vertice (tra cui, in maniera esemplificativa e non esclusiva, il Rettore/Prorettore, i Vicerettori, i Direttori di Dipartimento, il Direttore Generale, i Responsabili di Area/Servizio) all'intero personale o a suoi sottoinsiemi, con contenuti legati alla funzione svolta da ciascun soggetto.
Le liste istituzionali vengono create dinamicamente e in modo gerarchico rispetto alla struttura di afferenza, in modo da registrare tutti gli indirizzi di posta elettronica relativi a tutti i ruoli del personale strutturato e degli studenti implementati sul sistema di Identity Manager e su UNIDB.
È possibile quindi creare, a livello complessivo, le seguenti liste apicali:

- Personale docente e ricercatore;
- Personale tecnico, amministrativo e bibliotecario;
- Dottorandi;
- Assegnisti
- Studenti.

L'invio delle comunicazioni mediante le liste di distribuzione sopraindicate è autorizzato solo ai seguenti soggetti:

- Organi di governo e collegiali
- Dirigenti.

Qualsiasi ulteriore soggetto che intenda inviare una comunicazione ad una lista di distribuzione apicale, dovrà chiedere l'autorizzazione al Direttore generale il quale, entro 3 giorni dal ricevimento della richiesta, valuterà la rispondenza della comunicazione con i fini istituzionali propri dell'Ateneo e l'opportunità di utilizzare canali di distribuzione alternativi. Entro tale termine viene comunicata al richiedente l'eventuale impossibilità a concedere l'autorizzazione, specificandone i motivi del rigetto.

9.5.2 Liste di struttura

Le liste di struttura sono liste di distribuzione non apicali e il loro uso può essere reso disponibile per comprovate esigenze di servizio di singole strutture d'Ateneo (Aree, uffici, Dipartimenti ecc.).

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

Responsabile del corretto utilizzo della lista di distribuzione è il responsabile della struttura richiedente o suoi eventuali delegati.
È possibile la creazione di ulteriori liste di distribuzione di struttura a supporto degli uffici amministrativi dell'Ateneo, riguardanti specifici raggruppamenti omogenei del personale (formazione, carriera, livello di categoria, gruppi di lavoro, etc.) dalle liste istituzionali.

9.5.3 Liste di servizio

Le liste di servizio sono mailing-list create su specifica richiesta da parte degli uffici, organi e sigle di Ateneo, Associazioni, Enti convenzionati con l'Università degli Studi di Palermo, etc.
L'attivazione viene concessa dal Settore preposto dietro apposito nulla-osta del Direttore Generale, al quale va indirizzata la richiesta, completa delle motivazioni e del nominativo e indirizzo email dell'amministratore della lista.
Nelle liste di servizio, sebbene moderate dall'amministratore, tutti i membri possono sottoscrivere una spedizione a tutti gli altri membri della lista stessa.
Per tali ragioni, l'amministratore o moderatore è responsabile, ai fini amministrativi, civili e penali, del corretto utilizzo della stessa; autorizza le spedizioni ritenute opportune e scarta quelle ritenute non opportune; mantiene aggiornata la lista attraverso un controllo periodico della validità dell'e-mail registrata. Le liste di servizio devono permettere agli utenti o membri di esercitare il diritto di cancellazione. Tale diritto prevede che l'amministratore non potrà nuovamente inserire lo stesso indirizzo senza esplicita richiesta del titolare.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

10. Sistemi di comunicazione Sincrona

L'Ateneo, al fine di rispondere ai più moderni bisogni di comunicazione e interazione per l'intera comunità universitaria, può adottare sistemi di comunicazione sincrona per fornire agli utenti servizi innovativi quali mobilità, presenza, instant-messaging, messaggeria unificata, operatore automatico, rubrica on-line, conference call. Tali servizi dovranno essere resi disponibili indipendentemente dalla localizzazione e in pieno regime di mobilità sia in ambito intra che inter-ateneo, sfruttando tecnologie di trasmissione wireless/mobile e logiche di autenticazione federata (EduRoam, IDEM etc.).

10.1 Sistema VoIP

L'Ateneo adotta un sistema di comunicazione sincrona implementando una soluzione VoIP Open source basata sul software Asterisk PBX, utilizzando in rete apparati digitali di telefonia che permettono la gestione delle chiamate voce sulla rete IP su standard H.323 e SIP (Session Initiation Protocol) sia su UDP che su TCP.
Il protocollo H323, usato come protocollo per la comunicazione voce in tempo reale su IP, presiede a tutte le funzioni base di controllo di una chiamata: instaurazione e terminazione della sessione, operazioni di segnalazione, tono di chiamata, chiamata in attesa, trasferimento, identificazione del chiamante etc…. Mentre il protocollo SIP viene usato per la segnalazione e il controllo di sessioni multimediali, H.323 delinea un'architettura completa per lo svolgimento di conferenze multimediali, comprendente la definizione dei formati di codifica a livello applicativo, la definizione di protocolli per la segnalazione e il controllo, per il trasporto dei flussi audio, video e dati e per la gestione degli aspetti di sicurezza, tutto ciò con riferimento ad architetture di rete locali.
Il servizio è monitorato e curato dal Settore preposto e fornisce una o più numerazioni a tutti gli apparati telefonici fisici, in relazione all'utenza e/o all'ufficio/struttura di appartenenza.
È cura del settore preposto monitorare i flussi di chiamata secondo le direttrici di traffico su rete RTG locale/nazionale, cellulare e internazionale, configurando opportuni avvisi sui tempi e i periodi di chiamata individuale e i periodi complessivi per mese.
Su apposito registro di inventario, ad ogni apparato telefonico fisico devono essere associati: la rete IP, il responsabile, la struttura di riferimento (come da organigramma) e un titolare a cui assegnare il numero.
I titolari e i responsabili di struttura sono tenuti a utilizzare i servizi VoIP nel rispetto delle norme dell'Amministrazione pubblica.
L'utente, dotato di terminale VoIP collegato su rete IP al centralino dell'Ateneo, si presenta sulla rete telefonica generale (PSTN) con un numero di telefono del piano di numerazione nazionale (PNN) assegnato all'ateneo da un operatore telefonico; come previsto dalla normativa vigente (delibera 11/06/CIR) gli utenti devono essere informati di ogni limitazione connessa alla localizzazione delle chiamate di emergenza e alla disponibilità del servizio nel caso di utilizzo nomadico dei servizi VoIP offerti dall'ateneo nell'ambito dei suoi scopi istituzionali.
Per tale motivo, il sistema VoIP non deve essere implementato su apparati o procedure di sicurezza (sistemi antincendio, allarme intrusione, sistemi antipanico), o in strutture a rischio elevato (laboratori, magazzini, sale operatorie, strutture sanitarie) ogni struttura deve avere almeno un accesso RTG per le chiamate di sicurezza in assenza di rete dati e/o fornitura elettrica.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

Alle chiamate VoIP verso PSTN si applicano le limitazioni d'uso della rete telefonica eventualmente imposte dal responsabile di struttura dall'Ateneo alle diverse categorie di utenti.
I terminali VoIP devono essere logicamente associati alla rete wired dell'Ateneo, o essere connessi al centralino (PBX) VoIP attraverso un canale di comunicazione sicuro (VPN).
L'associazione del terminale VoIP al centralino dell'Ateneo deve richiedere l'autenticazione dell'utente attraverso una coppia di credenziali fornite al terminale in modalità di provisioning automatico. Solo su esplicita e motivata richiesta del titolare il Settore preposto può rilasciare una coppia di credenziali per abilitare altri apparati e/o client software.
Le chiamate entranti da rete PSTN (dirette o in selezione passante) devono poter essere ricevute su terminali VoIP in modo trasparente al chiamante: gli utenti e i servizi istituzionali devono poter essere raggiunti ai numeri telefonici geografici ad essi associati alla struttura/ufficio di appartenenza. Le chiamate uscenti verso rete PSTN effettuate da terminali VoIP devono presentarsi al ricevente con un numero del piano di numerazione nazionale assegnato all'Ateneo.
Per le chiamate in uscita non risposte alla numerazione mobile, il sistema VoIP deve consentire al chiamato di conoscere l'interno del chiamante effettuando la richiamata del numero.
L'Ateneo deve mettere in atto tutte le misure previste dalla normativa vigente, in fatto di audit e conservazione dei log, necessarie a fornire supporto all'Autorità Giudiziaria in materia di tracciamento del traffico e di identificazione degli utenti che usufruiscono del servizio VoIP, anche per le chiamate interne.
Per facilitare e incentivare la comunicazione su reti IP con gli altri Atenei, il sistema VoIP adotta soluzioni tecniche che supportano il protocollo ENUM e aderisce all'iniziativa NRENUM.
Gli interni vengono assegnati direttamente a tutto il personale docente e TAB con rapporto a tempo indeterminato, mentre, su richiesta di un responsabile, è possibile assegnare interni ad uffici o strutture. Tutti gli interni assegnati faranno parte di specifiche rubriche che verranno pubblicati sul portale di Ateneo.
Non è possibile istallare terminali VoIP in autonomia o non conformi alle specifiche tecniche rilasciate dal supporto VoIP del Settore preposto. Particolare attenzione deve essere prestata agli apparati citotelefonici istallati in esterno che permettono la possibilità di chiamare gli interni o effettuare azioni dirette sulla base di una chiamata VoIP. Le configurazioni di tali apparati in rete con possibili servizi web, ssh, IPcam istallati, devono essere registrate in conformità alle misure espresse dal GDPR.
I costi relativi all'acquisto, installazione, manutenzione ed esercizio degli apparati VoIP sono a carico delle strutture richiedenti.
Tutti i costi relativi al traffico RTG dovranno essere rendicontati alle singole strutture apicali e ogni titolare dovrà poter visionare il proprio traffico telefonico nel rispetto delle norme sulla privacy.
Le richieste di attivazioni dovranno pervenire attraverso apposita istanza elettronica al Settore preposto, che assegnerà il relativo numero interno.
Il numero interno è assegnato univocamente ad un titolare, tale numero segue la persona fisica nel cambio di afferenza di struttura e/o ufficio; sarà cura degli AdS informare il Settore preposto della mappatura del terminale nella nuova struttura.

10.2 Sistema di VideoConf

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it

L'Ateneo mette a disposizione di tutti gli utenti della rete GARR il servizio VideoConf per la comunicazione audio-video tra sedi diverse, dovunque esse siano, anche se non tutte connesse alla rete GARR.
La partecipazione dell'Ateneo alla federazione IDEM consente, utilizzando le proprie credenziali, di prenotare una stanza virtuale dove poter effettuare una riunione tra più utenti. I partecipanti alla riunione virtuale possono essere collegati su una rete qualsiasi (purché in grado di soddisfare i requisiti tecnici minimi richiesti). La conferma della prenotazione avviene via e-mail, dove è possibile trovare tutte le istruzioni per il collegamento, nel giorno e all'orario stabilito, alla stanza virtuale. Tale e-mail di conferma deve essere inoltrata a tutti i partecipanti, i quali possono collegarsi alla stanza virtuale utilizzando il loro terminale di videoconferenza. Vconf è anche accessibile dal servizio VoIP GARR e, in modalità solo audio e con numero di accessi limitato, dal servizio telefonico tradizionale. Il servizio VideoConf utilizza sistemi di videoconferenza su protocollo H323. Esso garantisce l'interoperabilità attraverso una sala regia e un server di videostreaming di Ateneo.
Per effettuare una comunicazione audio/video sulla rete, è necessario disporre di un terminale di videoconferenza dotato di microfono, casse audio e, opzionalmente, telecamera. E' possibile utilizzare: terminali hardware, ovvero terminali di tipo set-top-box, gestibili tramite l'utilizzo di un telecomando e che forniscono una dotazione completa per l'impiego in sale di medie/grandi dimensioni; è anche possibile l'utilizzo di terminali software, ovvero di PC con software di videoconferenza, utilizzando i dispositivi multimediali collegati al PC (telecamera, microfono e casse).

10.3 Utilizzo dei social network

L'Ateneo, per fini di comunicazione istituzionale, utilizza i principali social network attraverso un proprio account gestito dal responsabile degli uffici preposti alla comunicazione istituzionale.
L'uso dei social network da parte di tutto il personale docente e TAB di Ateneo, utilizzando la rete dell'Università, è consentito per gli scopi strettamente correlati al proprio ruolo e alle funzioni istituzionali dell'Università degli Studi di Palermo.

Settore Infrastrutture e Servizi ICT
Viale delle Scienze Ed. 11 – 90128 Palermo – Italy
email: servizi.sia@unipa.it