REGOLAMENTO PER L'ATTRIBUZIONE DI UTENZE E ACCESSO A SERVIZI DI RETE E POSTA ELETTRONICA DI ATENEO

(emanato con Decreto Rettorale prot. n. 41762 del 2 luglio 2019)
(modificato con Decreto Rettorale n. 530/2025, prot. n. 92702 del 7 novembre 2025, previa approvazione del Senato Accademico con delibera n. 105/2025 del 29 ottobre 2025 e parere favorevole del Consiglio di Amministrazione con delibera n. 216/2025 del 29 ottobre 2025)

Sommario

TITOLO I – UTENTI DI ATENEO

Art. 1 – Definizioni

1. **Strutture:** si intendono le strutture dell'Amministrazione Centrale e le strutture didattiche, scientifiche e di servizio dell'Ateneo.
2. **Rete di Ateneo:** è la rete dati dell'Ateneo costituita dalle varie Reti Locali, logiche e fisiche, e che interagisce con la rete pubblica di telecomunicazioni attraverso la connessione con la rete del consorzio GARR.
3. **Rete GARR**: è la rete italiana della ricerca a cui la Rete di Ateneo è collegata e tramite la quale avviene il collegamento alla rete Internet.
4. **Credenziali di Ateneo:** sono le credenziali elettroniche di autenticazione, in genere costituite da nome utente e password, rilasciate dall'Area Infrastrutture e Servizi Informatici (AINF) e che identificano univocamente un soggetto nell'ambito dell'Ateneo.
5. **Servizio di rete**: si intendono i servizi erogati tramite la Rete di Ateneo a utenti in possesso delle necessarie risorse. In particolare, sono servizi di rete l'accesso stesso alla Rete di Ateneo (wired o wireless) e il servizio di posta elettronica di Ateneo.
6. **Gestore di un servizio** è in genere il responsabile della Struttura che eroga il servizio. La

funzione di gestore dei servizi centralizzati di rete dell'Ateneo è svolta dall'Area Infrastrutture e Servizi Informatici (AINF)
7. **ZTUA (Zero Trust User Access):** la Policy di Sicurezza Utenti dell'Ateneo, che definisce criteri, regole e controlli per la gestione delle identità digitali e degli accessi ai sistemi informatici secondo il modello Zero Trust, basato sulla verifica continua dell'identità e sul principio di accesso minimo necessario. La ZTUA costituisce allegato tecnico del presente regolamento e può essere aggiornata con provvedimento del Direttore Generale qualora necessitasse di adeguamenti tecnici.

Art. 2 – Principi, finalità e ambito applicativo

1. Il presente regolamento recepisce la vigente normativa in materia di sicurezza informatica, trattamento e protezione dei dati personali e criminalità informatica, nonché le indicazioni degli organi di riferimento nazionali ed internazionali e la politica di uso della rete nazionale della ricerca (consorzio GARR). Pertanto le norme relative all'uso della rete GARR emanate ed emendate dai responsabili della rete GARR fanno parte integrante del presente regolamento.
2. Il presente regolamento è basato sui seguenti principi di carattere generale:
a) responsabilità: l'assegnazione di risorse, sia essa diretta o a seguito di delega, è subordinata alla assunzione di responsabilità da parte del soggetto assegnatario, in ordine alle risorse assegnate ed alle attività di rete ad esse riconducibili;
b) tracciabilità: le attività che danno origine a traffico esterno devono essere imputabili a soggetti noti e identificabili;
c) autonomia: le attività che possono generare esclusivamente traffico interno rientrano nell'ambito regolamentare delle singole Strutture.
3. Il presente regolamento ha lo scopo di:
a) definire compiti e responsabilità dei soggetti che partecipano alla gestione e all'utilizzo della Rete di Ateneo;
b) disciplinare l'assegnazione e l'impiego delle risorse, al fine di garantirne un uso legale, omogeneo e corretto;
c) determinare le modalità di erogazione dei servizi di rete e stabilire le relative norme per l'accesso e l'uso.
4. Il presente regolamento si applica a tutte le Strutture e a tutti i soggetti, siano essi utenti finali o gestori di un servizio, ai quali l'Ateneo ha assegnato una o più risorse. Il regolamento è applicato anche ai soggetti esterni all'Ateneo che, a seguito di specifici accordi o convenzioni, utilizzano le risorse di Ateneo o svolgono attività a esse collegate. L'uso delle credenziali è disciplinato dal presente regolamento e dalla Policy di Sicurezza Utenti (ZTUA) di Ateneo, allegata al presente documento.

Art. 3 – Utenti di ateneo

1. I soggetti che appartengono alle seguenti categorie, fino a quando permangono i requisiti di appartenenza, hanno titolo ad accedere ai servizi di rete, di posta e all'utilizzo delle risorse:
a) Utenti interni standard
1) Docenti e ricercatori di ruolo
2) Personale tecnico-amministrativo
3) Studenti iscritti ai corsi di laurea
4) Dottorandi di ricerca

5) Specializzandi
6) Assegnisti di ricerca
7) Titolari di borse di studio
Tutte queste sottocategorie, in termini di sicurezza, rientrano nelle regole definite per gli **utenti interni standard** dalla Policy di sicurezza utenti (ZTUA).
b) Utenti interni privilegiati
Personale con ruoli amministrativi o di gestione dei sistemi e servizi informatici di Ateneo.
Questi soggetti, in termini di sicurezza, rientrano nelle regole definite per gli **utenti interni privilegiati** dalla Policy di Sicurezza Utenti (ZTUA).
c) Utenti esterni
Visiting professor, studenti e docenti ospiti, collaboratori, fornitori e service provider, sulla base di specifici accordi o autorizzazioni.
Tutte queste sottocategorie, in termini di sicurezza, rientrano nelle regole definite per gli **utenti esterni** dalla Policy di Sicurezza Utenti (ZTUA).
d) Account shared e account di servizio
Account impersonali, condivisi o destinati al funzionamento e alla configurazione di applicazioni o sistemi, gestiti dall'Area Infrastrutture e Servizi Informatici.
Tali account, in termini di sicurezza, rientrano nelle regole definite per gli **account condivisi (shared)** e **account di servizio** dalla Policy di Sicurezza Utenti (ZTUA).

Art. 4 – Credenziali elettroniche di Ateneo

1. Le Credenziali elettroniche di Ateneo costituiscono l'identità digitale primaria rilasciata dall'Università di Camerino e sono costituite da un account di Active Directory (AD) e dalla relativa password personale. Esse consentono l'accesso ai sistemi informatici e ai servizi digitali dell'Ateneo, nel rispetto delle regole tecniche e organizzative definite dalla Policy di Sicurezza Utenti (ZTUA)**.**
2. L'account di Active Directory identifica in modo univoco l'utente nei sistemi dell'Ateneo e rappresenta la base di autenticazione per l'accesso a:
a. piattaforme e applicazioni di Ateneo (didattiche, amministrative, gestionali);
b. servizi del personale (cedolino, documenti fiscali, previdenziali e dichiarativi);
c. portali degli studenti ed ex studenti (carriera, certificati, attestati, documenti di segreteria);
d. sistemi di rete e infrastrutture informatiche integrati con l'autenticazione centralizzata.
3. L**'**account di Active Directory è distinto dalla casella di posta elettronica eventualmente associata all'utente. La disattivazione o la cancellazione della casella di posta non comporta automaticamente la disattivazione dell'account di AD, che può continuare ad essere utilizzato per accedere ai servizi indicati al comma 2. La durata della casella di posta è disciplinata separatamente dall'articolo 10 del presente regolamento.
4. La creazione, gestione, conservazione e revoca delle Credenziali di Ateneo è di competenza dell'Area Infrastrutture e Servizi Informatici (AINF**)**, che provvede all'autenticazione centralizzata e alla protezione dei dati nel rispetto della normativa vigente e della Policy ZTUA.
Le credenziali sono conservate in forma cifrata e non sono visibili in chiaro.
5. La validità dell'account di Active Directory è fissata come segue:
a. per il personale docente, ricercatore, tecnico-amministrativo, assegnisti, borsisti e

collaboratori: alla data di cessazione del rapporto con l'Ateneo;
b. per gli studenti ed ex studenti: 5 anni dopo la cessazione della carriera universitaria o il conseguimento del titolo di studio;
c. in ogni momento, in caso di uso non conforme, compromissione delle credenziali o violazione del presente regolamento.
6. Al termine del periodo di validità indicato al comma 5, l'account di Active Directory viene disattivato e reso inaccessibile all'utente. L'utente viene informato preventivamente della disattivazione e può esportare i propri dati o documenti contenuti nei servizi associati secondo le procedure predisposte dall'Ateneo.
7. La cancellazione definitiva dell' account potrà essere effettuata dall'Area Infrastrutture e Servizi Informatici (AINF) secondo tempi e modalità da essa stabiliti in occasione di manutenzioni programmate del sistema di autenticazione nel rispetto dei principi di sicurezza, pertinenza e minimizzazione del trattamento dei dati personali, nonché degli obblighi di conservazione amministrativa e comunque non prima di 5 anni dalla disattivazione
L'utente viene informato preventivamente con largo anticipo (6 mesi) della cancellazione definitiva e può esportare i propri dati o documenti contenuti nei servizi associati secondo le procedure predisposte dall'Ateneo.
8. I log di autenticazione e le informazioni di tracciabilità relative agli account disattivati sono conservati per il tempo strettamente necessario a garantire la sicurezza dei sistemi, la verifica degli accessi e l'adempimento di obblighi amministrativi o di legge.

Art. 5 – Servizi associati alle Credenziali di Ateneo

1. Le Credenziali elettroniche di Ateneo, costituite dall'account di Active Directory e dalla relativa password personale, consentono l'accesso a un insieme di servizi digitali integrati, gestiti o federati dall'Università di Camerino. Rientrano tra i servizi associati alle Credenziali di Ateneo:
a) i servizi di rete di Ateneo, inclusi l'accesso alla rete cablata, wireless e ai servizi VPN, normati nel TITOLO II del presente regolamento;
b) la posta elettronica istituzionale, erogata nei domini *@unicam.it* e *@studenti.unicam.it*, normati nel TITOLO III del presente regolamento.
c) la suite Google Workspace,
d) il servizio Microsoft OneDrive for Business, parte integrante dell'infrastruttura Microsoft 365 di Ateneo, utilizzato per l'archiviazione e la condivisione sicura dei documenti;
e) eventuali piattaforme e applicazioni interne o federate che prevedano l'autenticazione tramite l'identità digitale di Ateneo (ad esempio portali del personale, carriera studenti, segreterie online, sistemi gestionali e didattici).
2. L'accesso ai servizi elencati è subordinato alla validità delle Credenziali di Ateneo e alla permanenza del rapporto con l'Ateneo, secondo quanto previsto dall'articolo 4.

Art. 6 – Obblighi dell'utente

1. Le Credenziali di Ateneo verranno rilasciate agli utenti di cui al punti a) dell'art. 3 nel momento in cui le relative posizioni giuridiche verranno formalmente regolarizzate nel sistema informatico di Ateneo e a seguito della sottoscrizione di un verbale di rilascio. Le restanti tipologie di utenti al punto c) e d) dell'art. 3 che intendano accedere a un servizio di rete devono presentare al Responsabile della Struttura di riferimento richiesta di assegnazione

delle risorse necessarie. Una volta validata dal Responsabile della Struttura, la richiesta andrà trasmessa all'Area Infrastrutture e Servizi Informatici (AINF). Sia il documento riguardante gli utenti di cui ai punti a) sia la richiesta che devono presentare le tipologie di utenti c) e d) saranno conformi a quanto richiesto dal comma 2 del presente articolo e corredati degli elementi che consentano al gestore di effettuare la procedura di identificazione, prevista dal principio di tracciabilità di cui alla lettera b) dell'art. 2.2.

2. L'utente, sottoscrivendo il documento o la richiesta di cui al comma precedente:

a) assume, in applicazione del principio di responsabilità enunciato alla lettera a) dell'art. 2.2, ogni responsabilità penale e civile in ordine all'uso e cura delle risorse assegnate e a tutte le attività di rete relative al loro impiego, fino alla loro scadenza o formale restituzione o fino alla notifica della loro revoca per uso non corretto o non conforme al presente regolamento. Nel caso particolare che le risorse assegnate consentano attività di rete solo a seguito di un processo autorizzativo, comunque preceduto da autenticazione, la responsabilità dell'utente, relativamente a tali attività, è da intendersi limitata ai soli intervalli temporali di utilizzazione delle risorse certificati dal gestore del servizio di autorizzazione;

b) si impegna a rispettare la vigente normativa, la Acceptable Use Policy del consorzio GARR (https://www.garr.it/it/regole-di-utilizzo-della-rete-aup) e il presente regolamento, a utilizzare le risorse assegnate e la Rete di Ateneo ai soli fini istituzionali e in maniera da non recar danno o pregiudizio all'Ateneo o a terzi e a non interferire con l'utilizzo dei servizi di rete da parte di altri utenti. Si impegna inoltre a non utilizzare le risorse eventualmente pervenute nella propria disponibilità a seguito di una procedura non conforme con quanto previsto dal presente articolo, fatto salvo quanto espressamente previsto a tale riguardo dall'art. 10.3, ovvero quelle scadute, formalmente restituite o revocate, anche se regolarmente assegnate ai sensi del presente regolamento;

c) prende atto delle indicazioni che vi sono riportate e relative alla scadenza, uso e cura delle risorse assegnate e alle azioni da intraprendere nel caso di perdita, violazione o sottrazione;

d) prende atto che, nel caso di uso non corretto o non conforme al presente regolamento, il gestore del servizio può disporre la revoca delle risorse assegnate, dandone comunque notifica all'interessato;

e) consente il monitoraggio e la misura delle attività di rete generate dalle risorse che gli sono state assegnate, al fine di garantirne funzionalità e affidabilità e nel rispetto del principio di pertinenza e non eccedenza, secondo quanto previsto dalla normativa vigente;

f) solleva il gestore del servizio e l'Ateneo da ogni responsabilità e obbligazione in relazione agli eventuali danni che potrebbero derivargli da guasti o malfunzionamenti degli apparati di gestione e, in generale, dall'erogazione del servizio stesso.

3. Quanto previsto dal precedente comma 2, con particolare riferimento al rispetto della Acceptable Use Policy del consorzio GARR, si applica anche alle tipologie di utenti provenienti da istituzioni che aderiscono al servizio **EDUROAM**, servizio che permette agli utenti in mobilità presso altre organizzazioni di accedere in modo semplice e sicuro alla rete wireless dell'Ateneo usando le medesime credenziali fornite dalla propria organizzazione. La necessaria presa visione del presente regolamento per queste tipologie di utenti è a cura del responsabile della struttura cui fanno riferimento.

TITOLO II – ACCESSO AI SERVIZI DI RETE

Art. 7 – Ruolo dei soggetti che concorrono alla gestione della Rete di Ateneo

1. I soggetti che partecipano alla gestione della Rete di Ateneo, fatte salve le competenze degli Organi centrali dell'Ateneo, sono: **il Delegato del Rettore alla Rete GARR, l'Area Infrastrutture e Servizi Informatici (AINF)**
2. **Il Delegato del Rettore alla Rete GARR** cura i rapporti con il consorzio GARR, si occupa della pianificazione e ottimizzazione delle risorse della rete di Ateneo e dell'accesso alla Rete GARR, avvalendosi del contributo dell'Area Infrastrutture e Servizi Informatici (AINF).
3. **L'Area Infrastrutture e Servizi Informatici (AINF)**, secondo quanto previsto dalla "Nuova organizzazione interna delle strutture tecnico amministrative di Ateneo" emanata con Disposizione del Direttore Generale prot. n. 48331 del 11/7/2022 provvede a gestire:
a) le Reti Locali e la Rete di Ateneo, predisponendone le soluzioni tecnologiche e organizzative;
b) lo spazio di indirizzamento relativo alle risorse di rete e di indirizzamento dell'Ateneo;
c) il servizio centralizzato di autorizzazione di Ateneo;
d) il servizio centralizzato di generazione delle Credenziali di Ateneo e di autenticazione di Ateneo;
e) la conservazione, nel rispetto della normativa e delle raccomandazioni del Garante, delle informazioni contenenti l'associazione tra identità elettronica dell'utente, identificativo della risorsa di rete o di indirizzamento utilizzata e intervallo temporale di utilizzazione della risorsa stessa
f) il servizio di posta elettronica di Ateneo;
g) i servizi di rete per conto delle Strutture;
h) servizi applicativi di carattere generale (es. servizi di teleconferenza, servizi di erogazione della didattica in modalità streaming).
L'Area Infrastrutture e Servizi Informatici (AINF), al fine di garantire la continuità dei servizi e la operatività ed efficienza della rete (come previsto dall'art. 7) può effettuare interventi tecnici di natura ordinaria o straordinaria, che comportino anche riduzione o interruzione dei servizi, con lo scopo di limitare gli effetti di un evento dannoso per la rete o per gli altri utenti e di ripristinare l'efficienza dei servizi nel più breve tempo possibile.

Art. 8 – Obblighi dei gestori dei servizi di rete

1. I servizi di rete sono ispirati a principi di sicurezza, affidabilità ed efficienza. Tutti i soggetti che, direttamente o a seguito di delega, gestiscono servizi di rete erogati tramite la Rete di Ateneo si impegnano a:
a) assicurare, con riferimento alle attività oggetto del servizio, l'osservanza della vigente normativa, la Acceptable Use Policy del consorzio GARR e il presente regolamento;
b) utilizzare i dati di pertinenza o di proprietà dell'utente ai soli fini della gestione o erogazione del servizio e adoperarsi al meglio per proteggerne la riservatezza e l'integrità;
c) garantire la privacy dell'utente;
d) assicurare la continuità del servizio, fatte salve eventuali sospensioni dovute

all'ordinaria o straordinaria manutenzione e a eventi straordinari e imprevedibili;
e) provvedere all'aggiornamento tecnologico dei componenti hardware e software;
f) erogare i servizi in una forma agevolmente fruibile dall'utenza e fornire le indicazioni necessarie per un uso corretto.

Art. 9 – Accesso alla Rete di Ateneo

1. Il principio di tracciabilità, di cui alla lettera b) dell'art. 2.2, presuppone che le attività che danno origine a traffico esterno siano imputabili a soggetti noti e identificabili. A questo fine, l'accesso alla Rete di Ateneo (e di conseguenza a quella pubblica) è consentito secondo una delle seguenti modalità:
a) *autorizzazione basata su Credenziali di Ateneo*
La validazione delle Credenziali di Ateneo è effettuata dall'Area Infrastrutture e Servizi Informatici (AINF).. Le credenziali sono generate e conservate nell'ambito nell'infrastruttura Microsoft Active Directory di Ateneo, che verifica le autenticazioni degli utenti in fase di accesso all'utilizzo dei servizi di rete.
b) *uso strettamente personale di una risorsa di rete*
Per situazioni di particolari necessità, specie riguardo a risorse che supportano determinate attività elaborative (workstation di dipartimento, attrezzature di laboratorio, ecc.), può essere consentita una modalità di accesso alla Rete di Ateneo attraverso l'associazione permanente tra identità fisica e indicativo della risorsa di rete assegnata.

Art. 10 – Disattivazione dell'accesso alla Rete per gli studenti

1. Per gli studenti, l'accesso alla Rete di Ateneo, nelle sue componenti cablata, wireless e VPN, viene disattivato al termine del rapporto con l'Università di Camerino, indipendentemente dalla validità residua delle Credenziali di Ateneo.
2. La riattivazione dell'accesso potrà avvenire esclusivamente a seguito di una nuova iscrizione o di un rapporto attivo con l'Ateneo che ne preveda l'abilitazione.

Art. 11 – Attività vietate

1. Stante i principi richiamati nel Codice Etico e di Comportamento di Ateneo, è fatto espresso divieto di usare la rete:
a. In modo difforme da quanto previsto nel presente regolamento;
b. In modo difforme dalle regolamentazioni dettate dai responsabili della rete GARR;
c. In modo difforme da quanto previsto dalle leggi penali, civili e amministrative in materia di disciplina delle attività e dei servizi svolti sulla rete.
d. Per scopi incompatibili con le finalità e con l'attività istituzionale dell'Ateneo così come stabilito nello Statuto dell'Università;
e. Per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Ateneo;
f. Per commettere attività che violino la riservatezza di altri utenti o di terzi;
g. Per attività che influenzino negativamente la regolare operatività della rete o ne restringano l'utilizzabilità e le prestazioni per gli altri utenti;
h. Per attività che distraggano risorse per fini non istituzionali (persone, capacità, elaboratori);
i. Per attività che provochino trasferimenti non autorizzati di informazioni (software, basi dati, etc.);

j. Per attività che violino le leggi a tutela delle opere dell'ingegno.
k. Usare l'anonimato o servirsi di risorse che consentono di restare anonimi.
2. In caso di abuso, a seconda della gravità del medesimo, e fatte salve le ulteriori conseguenze
9
di natura penale, civile e amministrativa, potranno essere comminate sanzioni come previsto da Codice etico e di Comportamento di Ateneo.

TITOLO III – POSTA ELETTRONICA DI ATENEO

Art. 12 – Sistema di posta elettronica di Ateneo, assegnazione e revoca caselle di posta

1. La gestione del sistema di posta elettronica di Ateneo è di competenza dell'Area Infrastrutture e Servizi Informatici (AINF). Le autorizzazioni necessarie all'utilizzo del sistema, che permettono la gestione di una casella di posta elettronica per l'invio e la ricezione dei messaggi, sono basate sulle Credenziali di Ateneo, di cui all'art. 7.
2. Le caselle di posta elettronica istituzionali sono rilasciate in relazione al dominio di appartenenza dell'utenza:
a) per il dominio principale vengono utilizzati indirizzi nella forma *<indicativo>@unicam.it;*
b) per il dominio *studenti* vengono utilizzati indirizzi nella forma *<indicativo>@studenti.unicam.it.*
3. Agli utenti di cui all'Art. 3. lettere a) 1,2,4,5,6 sono assegnate caselle nel dominio *@unicam.it*
4. Agli utenti di cui all'Art. 3 lettere a) 3, 7 sono destinate caselle nel dominio *@studenti.unicam.it*
5. Le caselle di posta elettronica di cui al comma 2), appartengono alle seguenti tipologie:
a) *caselle di tipo personale*: vengono assegnate a soggetti che ne abbiano titolo ai sensi dell'art. 3.. La casella di tipo personale individua univocamente l'assegnatario. Il descrittore <indicativo> è composto in forma: *nome.cognome*, con le variazioni necessarie per risolvere i casi di omonimia.
b) *caselle di tipo impersonale*: sono utilizzate, in relazione alle funzioni svolte, da cariche istituzionali e da responsabili protempore di strutture, servizi, organizzazioni interne e associazioni dell'Ateneo. I titolari protempore delle caselle impersonali si impegnano, contestualmente al loro uso, a rispettare le clausole previste dall'art. 4.2, restando così esonerati dalle procedure di identificazione e di richiesta di assegnazione, in deroga a quanto previsto dall'art. 4.1. La casella di tipo impersonale individua univocamente il titolare protempore, la cui funzione è descritta dal campo <indicativo>.
6. Per quanto riguarda le caselle di tipo personale nel dominio **@unicam.it** assegnate in seguito all'instaurarsi di un rapporto di lavoro o collaborazione con l'Ateneo, resteranno nella disponibilità dell'assegnatario fino ai 12 mesi successivi alla data di cessazione di tale rapporto. A ridosso della cessazione del rapporto di lavoro o collaborazione con l'Ateneo, l'assegnatario deve trasferire al proprio responsabile di Struttura tutte le comunicazioni che possano essere di interesse per le attività istituzionali dell'Ateneo. Qualora persista a qualsiasi titolo un rapporto con l'Ateneo, l'assegnatario potrà far richiesta al proprio responsabile di struttura per il mantenimento oltre il periodo indicato.
7. Le caselle di posta elettronica assegnate nel dominio @studenti.unicam.it agli studenti iscritti a uno dei corsi di studio dell'Ateneo restano nella disponibilità degli assegnatari fino a quando risulta attiva almeno un'iscrizione riferita agli ultimi quattro anni accademici rispetto a quello in corso. Decorso tale periodo senza ulteriori iscrizioni o conseguimento

di un titolo di studio, la casella viene considerata inattiva e sono inviati alla stessa messaggi di preavviso relativi alla disattivazione. La disattivazione definitiva avverrà entro i successivi dodici mesi dall'invio del primo avviso, salvo rinnovo dell'iscrizione o riattivazione della carriera accademica. La disattivazione potrà inoltre essere disposta in qualsiasi momento in caso di uso non corretto o non conforme al presente regolamento.
8. Prima della disattivazione, per qualsiasi motivazione di cui ai commi precedenti, sarà inviata opportuna informativa all'utente finale con le informazioni per la procedura di esportazione dei dati e la data di disattivazione.
11
9. Il Sistema di posta elettronica prevede anche l'utilizzo di liste di distribuzione, attraverso le quali sono raggruppate caselle di posta elettronica secondo determinati criteri funzionali e informativi e a cui vengono recapitati di messaggi indirizzati alla lista di distribuzione.
L'Area infrastrutture e servizi informatici (AINF) provvede alla generazione di liste di distribuzione tra le quali :
a) liste di tipo generale adibite alla diffusione di informazioni di carattere istituzionale, sia di interesse generale che di servizio. L'iscrizione di un utente alle liste di tipo generale avviene automaticamente.
b) gruppi omogenei o funzionali o comunque personalizzati di utenti appartenenti alle categorie indicate nell'art. 3. Queste liste di gruppo sono attivate dietro motivata richiesta. La partecipazione alle liste di gruppo che non riguardano le funzioni istituzionali dell'Ateneo è nella disponibilità degli utenti.
La manutenzione e autorizzazione all'uso delle liste di distribuzione sono di pertinenza dei rispettivi proprietari, che in genere faranno riferimento alla Struttura o Servizio che ha inoltrato la richiesta di creazione.

Art. 13. - Fornitore del servizio

1. L'Ateneo dispone di caselle di posta e applicativi tramite piattaforme interne o esterne all'Ateneo. In caso di servizio esternalizzato l'utente è tenuto a prendere visione di questo Regolamento di Ateneo e delle policy e termini di utilizzo del fornitore esterno che integrano e non sostituiscono le vigenti norme nazionali, europee e locali.
2. L'Ateneo assicura la messa a disposizione dell'utente finale di una procedura di "takeout" per l'esportazione dei dati relativi al servizio di posta. L'esportazione consente agli utenti finali di avere un archivio dei propri dati permettendone l'importazione in altri ambienti di lavoro e/o applicazioni.

Art. 14. - Obblighi dell'utente finale

1. L'utente finale delle caselle di posta del Sistema di posta elettronica di Ateneo si impegna a:
a. conservare le credenziali di accesso personali, senza mai comunicarla a terzi;
b. notificare immediatamente all'Ateneo l'eventuale perdita di riservatezza esclusiva della password;
c. non divulgare informazioni riservate relative ad altri utenti finali di cui venisse a conoscenza;
d. non caricare, trasmettere, utilizzare, diffondere qualsiasi materiale che non possa essere legalmente distribuito in via telematica. L'utente finale è pienamente responsabile, anche penalmente, dei dati da lui inoltrati e gestiti attraverso i servizi offerti.

Art. 15. - Limiti di responsabilità e obblighi dell'Ateneo

1. L'Ateneo è tenuto indenne da qualsiasi danno, perdita, costo, responsabilità, nonché dagli oneri di spesa che dovessero derivare da atti, fatti, comportamenti illeciti o omissioni posti in essere dall'Utente finale nell'utilizzo dei servizi.
2. L'Ateneo può sospendere l'account dell'utente finale qualora venga a conoscenza:
a. di un utilizzo non conforme a quanto previsto dalla presente Regolamento e dalle norme di legge;
b. di accessi potenzialmente sospetti da parte di terzi;
12
c. di violazione dei termini di servizio del fornitore.
1. L'Ateneo non può ripristinare l'account di un utente sospeso per violazione dei termini di servizio del fornitore.
2. L'Ateneo può modificare i servizi offerti alla luce dell'evoluzione tecnologica e delle proprie scelte di gestione dei servizi medesimi.

TITOLO IV – NORME TRANSITORIE E FINALI

Art. 16. - Norme transitorie e finali

1. Il presente regolamento è pubblicato all'Albo dell'Università ed entra in vigore il giorno stesso della sua pubblicazione.
2. È parte integrante del presente Regolamento il documento tecnico "ZTUA – Zero Trust User Access - Policy di sicurezza".

Art. 16-bis. - Norme transitorie e finali per l'autenticazione 802.1X

1. Al fine di garantire una maggiore sicurezza informatica e nel rispetto delle Acceptable Use Policy (AUP) del consorzio GARR, l'Università di Camerino sta progressivamente implementando un sistema di autenticazione 802.1X basato su account e password personali per l'accesso alla rete cablata **(**Wired**).**
2. Fino al completamento del deploy del sistema di autenticazione 802.1X in tutti gli edifici Unicam, la responsabilità degli indirizzi IP utilizzati all'interno delle singole strutture resta in capo, come previsto dal precedente regolamento**,** ai rispettivi responsabili di struttura che sono tenuti a garantirne l'uso conforme al presente regolamento e alle policy di sicurezza di Ateneo.
3. I responsabili di struttura sono inoltre responsabili:
a) degli indirizzi IP fissi o statici assegnati a risorse Unicam non gestite direttamente dall'Area Infrastrutture e Servizi Informatici (AINF) (es. siti web, applicazioni, storage, dispositivi IoT);
b) delle eventuali aperture di porte sul firewall perimetrale dell'Ateneo richieste per tali risorse;
c) della gestione di eventuali eventi di sicurezza o traffico malevolo riconducibili agli indirizzi IP sotto la loro responsabilità.
4. Al termine del periodo di transizione, con il completamento dell'implementazione del sistema 802.1X, le responsabilità di cui sopra saranno assorbite dal sistema di autenticazione centralizzato e dalle strutture tecniche competenti dell'Ateneo.