Università degli Studi di Ferrara

REGOLAMENTO PER LA DESIGNAZIONE DEGLI AMMINISTRATORI DI SISTEMA

Emanato con Decreto Rettorale Rep. 09/2025 Prot. n. 2239 del 8/01/2025
Entrato in vigore: 23 gennaio 2025

Sommario

Articolo 1. Oggetto del documento

1. Il presente regolamento descrive le modalità di designazione degli amministratori di sistema dell'Università degli Studi di Ferrara e i compiti ad essi assegnati.

   Per "amministratori di sistema" si intendono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad es. gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi[1].
2. Non rientrano in questa definizione coloro i quali, per scopi di didattica o di ricerca, gestiscano temporaneamente server, apparati di rete o software complessi qualora questi non

coinvolgano servizi essenziali o strategici dell'Università e non presentino rischi significativi in merito alla protezione dei dati personali, fermo restando la necessità di seguire le norme

[1] Definizione da provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" pubblicato sulla G.U. n. 300 del 24-12-2008

indicate nel “Regolamento d’uso delle risorse informatiche” e di ogni altra norma o regolamento interno che disciplini l’uso della rete e delle risorse informatiche dell’Ateneo.

3. Nell’ambito di questo documento si intendono per “referenti per i servizi IT dell’Ateneo” le persone, unità o strutture che per delega, incarico o posizione organizzativa hanno specifica competenza per il particolare servizio o ambito ICT come desumibile dalle indicazioni di accesso ai servizi pubblicate sul portale di Ateneo.
4. Tutte le cariche, professioni e titoli inerenti a funzioni nominate nel presente regolamento e declinate al genere maschile devono intendersi riferite anche al corrispondente termine di genere femminile.

Articolo 2. Ambito d’applicazione

1. Le linee guida si applicano a tutti gli amministratori di sistema che operano sui servizi sistemistici, infrastrutturali e applicativi che afferiscono al sistema informativo dell’Ateneo. A causa dell’interconnettività e dell’interdipendenza fra le componenti di un sistema informativo, i problemi di sicurezza su uno solo di essi propagano i loro effetti incidendo gravemente sulla sicurezza del sistema nel suo complesso. Per tale motivo tali linee guida sono recepite anche dagli enti che, a seguito di accordi o convenzioni, utilizzano il sistema informativo dell’Università.

Articolo 3. Procedura di designazione degli amministratori di sistema

1. Le designazioni sono effettuate dal Direttore Generale, su indicazione dei referenti per i servizi IT dell’Ateneo, per gli amministratori che devono operare presso la sede centrale e dal Direttore del Dipartimento o il Direttore del Centro presso cui l’amministratore deve svolgere le proprie funzioni per quello che riguarda le strutture decentrate. Il provvedimento di designazione degli amministratori di sistema deve indicare gli ambiti di operatività in funzione dei profili autorizzativi assegnati.
2. I referenti per i servizi IT dell’Ateneo e i Segretari amministrativi di Dipartimento, ciascuno per gli ambiti di propria spettanza, notificano il provvedimento all’interessato e, nel caso di dipendenti dell’Università, lo trasmettono per conoscenza alla struttura competente in materia di gestione del personale ai fini dell’aggiornamento del curriculum.

3. I Segretari amministrativi devono notificare le designazioni ai referenti per i servizi IT dell'Ateneo, che curano, ciascuno per la parte di propria competenza, la tenuta dell'elenco degli amministratori di sistema.
4. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare, il quale deve, quindi, fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008.

   Tale valutazione, per quello che riguarda il personale dipendente dell'Università, è effettuata dal Responsabile della designazione che, a tale scopo, si può avvalere della collaborazione dei referenti per i servizi IT dell'Ateneo.
5. L'amministratore di sistema designato, prima di prendere servizio nella funzione, deve inoltre dichiarare l'assenza di procedimenti disciplinari in corso e l'assenza di precedenti penali per i reati informatici di cui all'art. 615 ter del Codice Penale.Nei casi in cui il personale alle dipendenze di società esterne svolga funzioni di amministratore di sistema presso i Datacenter dell'Università, la società esterna di appartenenza deve effettuare la valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto ed effettuarne la designazione, fornendone all'Università attestazione formale. La società esterna deve inoltre essere preventivamente designata quale Responsabile del relativo trattamento.
6. I responsabili della designazione degli amministratori di sistema verificano annualmente la corretta designazione degli stessi e, inoltre, la sussistenza dei requisiti di capacità e di affidabilità del soggetto designato.
7. Nei casi non disciplinati dai paragrafi precedenti (ad esempio nei casi di fruizione di applicativi con modalità SaaS) la designazione degli amministratori di sistema è effettuata direttamente dai soggetti che erogano i servizi, i quali, designati Responsabili del trattamento per i servizi affidati, hanno l'obbligo di conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

   Tale onere deve essere espressamente indicato nella designazione del Fornitore quale Responsabile del trattamento dei dati personali, ai sensi e per gli effetti di cui all'art. 28 del Regolamento UE 2016/679.

Articolo 4. Registro digitale degli amministratori di sistema

1. I referenti per i Servizi IT di Ateneo mantengono, ognuno per quanto di propria competenza, un registro contenente i nominativi degli amministratori di sistema e l'ambito di operatività in funzione dei profili autorizzativi assegnati, individuando gli strumenti tecnologici più idonei per la sua gestione, conservazione e aggiornamento.
2. Il Registro degli amministratori di sistema contiene le seguenti macro categorie:
    a) **amministratori di dominio**: si tratta degli amministratori del dominio che consente l'accesso alle risorse e ai servizi informativi dell'Università;
    b) **amministratori di server**: si tratta degli utenti che hanno diritti amministrativi su uno o più server; a titolo esemplificativo rientrano in questa categoria gli utenti appartenenti al gruppo "Administrators" di uno o più server Windows o gli utenti di uno o più server Linux che attraverso il comando "sudo" possono impersonare l'utente "root";
    c) **amministratori di basi di dati**: si tratta degli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di "Data Definition Language";
    d) **amministratori di apparati di rete**: si tratta degli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni;
    e) **amministratori di apparati di sicurezza**: si tratta degli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus.
    f) **amministratori di sistemi software complessi**: si tratta degli utenti con privilegi di amministrazione di software applicativi o infrastrutturali che contengono diverse componenti hardware e software che interagiscono tra loro; esempi di sistemi software complessi sono i sistemi ERP, i sistemi di data warehouse, i sistemi di posta elettronica e i sistemi middleware.
3. I nominativi degli Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori sono messi a disposizione di questi attraverso il portale di comunicazione interna.

Articolo 5. Sistema di Access Log

1. I referenti per i Servizi IT di Ateneo tengono traccia degli accessi logici degli amministratori di sistema ai sistemi da essi amministrati. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo, non inferiore a un anno.

   A tale scopo è predisposto un sistema centralizzato di raccolta dei log dei sistemi, che garantisce le caratteristiche di completezza e inalterabilità richieste. Il sistema centralizzato di gestione dei log (log management) raccoglie i log di tutti gli accessi logici degli utenti (amministratori di sistema e non) dei sistemi sui quali siano stati designati amministratori di sistema e per i quali la tracciatura degli accessi sia tecnicamente possibile. Tale sistema è utilizzato inoltre per raccogliere e gestire i log di sicurezza di tutti i differenti sistemi che fanno parte del sistema informatico dell'Università.

   Pertanto, ogni qualvolta venga attivato un sistema su cui è necessario mantenere un "access log", occorre che l'amministratore di sistema competente concordi con il referente competente per lo specifico Servizi IT di Ateneo le modalità di integrazione ai fini della raccolta degli stessi. Allo stesso modo, una volta che il sistema viene dismesso, deve esserne comunicata la dismissione.
2. I referenti per i Servizi IT di Ateneo, verificano annualmente i log conservati al fine di verificare elementi di anomalia che possano far emergere criticità in termini di riservatezza, integrità e disponibilità delle informazioni.
3. Nel caso di applicativi gestiti direttamente da fornitori esterni queste attività possono essere demandate al fornitore stesso.

Articolo 6. Uso appropriato dei privilegi di amministratori

1. Al fine di prevenire attacchi informatici che sfruttino l'utilizzo di credenziali amministrative, è importante che gli amministratori di sistema utilizzino i privilegi amministrativi solo quando risulta indispensabile e che proteggano in maniera adeguata le loro credenziali amministrative.
2. Per tale motivo gli amministratori di sistema sono tenuti ad osservare le seguenti misure:

a) prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso;
b) tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa;
c) ove possibile, generare un'allerta quando viene aggiunta un'utenza amministrativa;
d) ove possibile, generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa;
e) ove possibile, utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza;
f) assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse;
g) le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per compiti amministrativi e deve essere possibile risalire in maniera univoca all'utente che le ha utilizzate e per quali scopi
h) evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio);
i) conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza;
j) se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette;
k) le credenziali amministrative non nominative di gestione dei sistemi non sono vincolate alle stesse regole delle credenziali nominative, non scadono dopo un periodo di inutilizzo, non vengono bloccate dopo un certo numero di tentativi errati, non hanno la password che scade e non ne viene richiesta la modifica al primo accesso. Perciò gli amministratori dei sistemi sono tenuti ad adottare politiche di modifica manuale delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato;
l) le credenziali amministrative non nominative create al solo scopo di avviare servizi sui server non devono poter effettuare l'accesso interattivo sui sistemi stessi o, ove ciò non fosse tecnologicamente possibile, deve essere comunque monitorato il loro utilizzo per scopi diversi rispetto all'ambito per cui sono state create;

m) le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via e-mail: in tali casi, è necessario convocare l'utente e fornirgli le credenziali verbalmente, oppure mediante un sistema di scambio informazioni sicuro;
n) le password non devono essere conservate in chiaro, né trasmesse su canali non cifrati .

Articolo 7. Sospensione dei privilegi

1. Nel caso in cui sia accertato che il comportamento colposo o doloso di un amministratore di sistema, in palese contrasto con le policy di sicurezza dell'Università, sia causa diretta o indiretta di un incidente di sicurezza e/o di una violazione dei dati personali, i soggetti che li hanno designati provvedono a sospendere i privilegi informatici ad esso assegnati finché le cause e le responsabilità effettive dell'incidente non siano state appurate.

Articolo 8 - Norme finali

Il presente Regolamento è emanato con decreto rettorale ed entra in vigore il 15° giorno successivo alla data di pubblicazione nell'Albo Online.