REGOLAMENTO AMMINISTRATORI DI SISTEMA

Compilato:	A. Troisi (Resp. Segreteria Affari Societari, Tutela Dati)	13/12/2024
Rivisto:	A. Trofin (Resp. Sistemi IT, Sicurezza)	13/12/2024
Autorizzato:	M. Bettini (Condirettore Generale e Direttore Operations)	13/12/2024

Versione:	1
Variante:	2 (Introdotto aggiornamento nell'articolo 4 per l'accettazione delle nomine pregresse)
Variante:	3 (Riviste le tipologie di Amministratore di Sistema e il profilo di autorizzazione che si intende affidare alla persona fisica)

INDICE

Principali modifiche alla versione precedente : prima edizione

INTRODUZIONE

ART. 1 DEFINIZIONE DI AMMINISTRATORI DI SISTEMA, COMPITI E RESPONSABILITÀ

Gli Amministratori di Sistema sono una categoria di operatori preposti all'esercizio dei sistemi informatici che, in funzione dei compiti ad essi assegnati, occupano i vertici della gerarchia di utenze, in termini di privilegi di accesso alle risorse informatiche e ai dati ivi custoditi.

Per tali motivi, il processo di attribuzione degli incarichi di Amministratore, così come la definizione dei relativi profili e permessi di accesso, riveste un carattere di estrema importanza per la sicurezza dei sistemi informatici e conseguentemente per la sicurezza delle informazioni personali a cui potrebbero accedere nello svolgimento dei propri compiti.

Il presente regolamento ha lo scopo di delineare e dettare le procedure di nomina e di attribuzione delle funzioni degli amministratori di sistema, nonché gli adempimenti in materia di protezione dei dati personali e, in particolare, l'adozione di specifiche misure e cautele in riferimento alle mansioni svolte dagli amministratori di sistema e dai soggetti (di profilo anche non strettamente tecnico-informatico) ad essi assimilabili, previsti dalla normativa vigente (Reg. UE 2016/679 e D. Lgs. n. 196/2003) e dai provvedimenti dell'Autorità Garante per la protezione dei dati personali (in particolar modo Provvedimento del Garante Privacy del 27 novembre 2008).

ART. 2 REQUISITI DI NOMINA

L'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

ART. 3 MODALITÀ DI NOMINA

La nomina deve essere individuale, per iscritto e deve riportare:

cognome e nome dell'Amministratore di Sistema nominato;

- le tipologie di Amministratore di Sistema e il profilo di autorizzazione che si intende affidare alla persona fisica;
- l'ambito di applicabilità.

In caso di variazione dell'assetto direttivo che per responsabilità sottoscrive gli atti di nomina, viene stabilito che in assenza di significative variazioni d'incarico, ogni precedente sottoscrizione rimane intesa come valida. Il Direttivo qualora non intendesse dare continuità al pregresso dovrà procedere con le attività di revoca.

La nomina generale rinvierà al perimetro di operatività, ai dettagli specifici delle funzioni, agli ambiti di applicabilità e alla responsabilità assegnata all'amministratore di sistema.

ART. 4 REVOCA DELLA NOMINA

Venis può revocare l'incarico di Amministratore di Sistema in caso di:

- violazione di quanto previsto dal presente documento;
- sopravvenuta mancanza dei requisiti ai sensi dell'art. 2;
- modifica del rapporto contrattuale di lavoro dell'Amministratore di Sistema.

In considerazione dei risvolti tecnici ma soprattutto di continuità ed affidabilità dei servizi, la revoca dell'incarico di un Amministratore di Sistema dovrà seguire la procedura indicata all'art. 5.

ART. 5 PROCEDURA DI REVOCA DEGLI AMMINISTRATORI DI SISTEMA

La revoca dell'incarico di un Amministratore di Sistema prevede le seguenti azioni da eseguire rigorosamente nell'ordine specificato:

- Nel caso non sia già esistente, creare un account amministrativo con lo stesso profilo di autorizzazione dell'Amministratore di Sistema da disabilitare, da assegnare al nuovo Amministratore di Sistema (sostituto);
- Disabilitare l'account dell'Amministratore di Sistema revocato;
- Comunicare la disabilitazione dell'account di Amministratore di Sistema e la revoca dell'incarico alla persona fisica.

ART. 6 FORMAZIONE ED AGGIORNAMENTO ANNUALE

Al fine di migliorare il livello di sicurezza della Società, l'Ufficio Tutela Dati organizza con cadenza annuale, sessioni di formazione ed aggiornamento sui temi della sicurezza nel trattamento dei dati e su temi specifici connessi ai compiti di amministrazione di sistema.

ART. 7 REDAZIONE E AGGIORNAMENTO DOCUMENTAZIONE

Gli estremi identificativi delle persone fisiche nominate Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un "Elenco degli Amministratori di Sistema" redatto, aggiornato e trasmesso all'Ufficio Tutela Dati. Tale documento sarà conservato presso la sede della Società e sarà sempre consultabile da parte del Responsabile della Protezione dei Dati nominato ai sensi dell'art. 37 Reg. UE 2016/679.

ART. 8 VERIFICA DELLE ATTIVITÀ DEGLI AMMINISTRATORI DI SISTEMA

L'Ufficio Tutela Dati – con il supporto del Responsabile della Protezione dei Dati personali - verifica con cadenza almeno annuale l'attività degli Amministratori di Sistema attraverso attività di audit, al fine di accertarne la conformità alle mansioni attribuite e la rispondenza alle misure organizzative, tecniche e di sicurezza ritenute adeguate.

ART. 9 REGISTRAZIONE DEGLI ACCESSI E DEGLI EVENTI

La Società del trattamento adotta sistemi idonei per garantire la registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema.

Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. I sistemi ed i dispositivi infrastrutturali ritenuti vitali e critici (per sensibilità dei dati contenuti o in quanto connessi direttamente alla continuità di servizi) dovranno prevedere anche la registrazione degli eventi (system log). Per un miglior controllo e governo dell'infrastruttura informatica della Società, sarà opportuno estendere la registrazione a tutti gli eventi di tutti i dispositivi collegati.

ART. 10 MONITORAGGIO E TRACCIABILITÀ

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a 6 mesi. Gli access log possono essere cancellati solamente alla scadenza dei 6 mesi.

La conservazione degli access log può essere on site o in outsourcing. In ogni caso dovrà essere in linea con le regole tecniche previste dal D. Lgs. n. 82/2005 e dalla relativa normativa di attuazione. Le modalità di registrazione, esportazione e conservazione dei log potranno essere dettagliate con apposita procedura operativa.

ART. 11 SALA SERVER

Gli ambienti denominati "Sala Server" sono considerati "Zona di massima sicurezza" e accessibile solamente agli Amministratori di Sistema individuati dalla Società o da personale interno di Venis da questi autorizzati e sorvegliati.

L'accesso al personale non autorizzato è vietato.

Tali ambienti sono chiusi e protetti da adeguati sistemi di sicurezza fisica.

Ogni singolo accesso del personale alla sala macchine deve essere registrato. Eventuali tecnici esterni devono essere identificati, autorizzati e registrati. In ogni caso il personale esterno può accedere solamente sotto stretta sorveglianza di un Amministratore di Sistema autorizzato o di personale interno di Venis da questi autorizzati.

ART. 12 DIVIETI E DISPOSIZIONI

La documentazione relativa all'infrastruttura di rete, alla configurazione dei sistemi o degli applicativi, alle impostazioni o abilitazioni degli utenti, deve essere conservata in luogo sicuro, preferibilmente non accessibile in rete. L'accesso a detta documentazione è consentito solamente al personale nominato Amministratore di Sistema, per il solo tempo necessario alla consultazione e all'aggiornamento.

TIPOLOGIA DI AMMINISTRATORI E PROFILI DI AUTORIZZAZIONE

Sono individuate le seguenti tipologie ed il relativo profilo di autorizzazione:

Tipologia	Livello Sicurezza	Ruolo	Profilo di autorizzazione
Enterprise Administrator	MAX	Livello più alto di autorizzazione nell'ambito della rete dell'Ente. Nel caso di singolo dominio le figure di Enterprise Administrator e Domain Administrator coincidono.	1. Autorizzato: 1. all'accesso completo a tutti i dati e a tutte le macchine appartenenti a tutti i domini della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli account ed abilitazione degli accessi agli Administrator di livello 0,1 e 2 di tutti i domini; 3. all'analisi e controllo dei log di tutte le macchine appartenenti a tutti i domini e dei dispositivi di tutta la rete (a meno di diversa ed esplicita configurazione).
Domain Administrator	0	Livello più alto di autorizzazione nell'ambito del singolo dominio della rete dell'Ente Nel caso di singolo dominio le figure di Enterprise Administrator e Domain Administrator coincidono.	2. Autorizzato: 1. all'accesso completo a tutti i dati ed a tutte le macchine appartenenti ad un singolo dominio della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli account e all'abilitazione degli accessi agli Administrator di livello 0,1 e 2 del solo dominio di appartenenza; 3. all'analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e dei dispositivi della porzione di rete gestita (a meno di diversa ed esplicita configurazione).
Server Administrator	1	Amministratore di un singolo sistema server.	3. Autorizzato: 1. all'accesso completo al sistema ed ai dati contenuti nel server (a meno di diversa ed esplicita configurazione); 2. a compiere qualsiasi operazione sistemistica e di modifica della configurazione del server; 3. all'analisi e controllo dei log.
Account Administrator	1	Amministratore degli account utente per il solo dominio di competenza.	4. Autorizzato: 1. alla creazione/disabilitazione degli account utente; 2. all'assegnazione del profilo di autorizzazione all'account utente.

Network Administrator	1	Amministratore dell'infrastruttura di rete e di comunicazione.	5. Autorizzato: 1. all'accesso completo ai dispositivi e linee di comunicazione dati; 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di comunicazione dati; 3. all'analisi e controllo dei log e del traffico dati.
Security Administrator	1	Amministratore dei dispositivi di sicurezza.	6. Autorizzato: 1. all'accesso completo ai dispositivi di sicurezza (es. Firewall, Antivirus, Log Management, Traffic analyzer); 2. a compiere qualsiasi operazione di modifica della configurazione dispositivi di sicurezza; 3. all'analisi e controllo dei log.
Database Administrator	1	Amministratore di un database server o di una singola istanza di database.	7. Autorizzato: 1. all'accesso completo al motore del database ed ai dati memorizzati; in casi particolari è possibile autorizzare anche la singola istanza di database; 2. a compiere qualsiasi operazione di modifica della configurazione e degli schemi dei database; all'analisi e controllo dei log; 3. a predisporre e rendere funzionanti le copie di sicurezza.
Service Administrator	1	Amministratore dei singoli servizi applicativi.	8. Autorizzato: 1. Alla gestione, modifica delle configurazioni, stop/start del singolo servizio o applicazione; 2. all'analisi e controllo dei log specifici del servizio o applicazione.
Backup Administrator	1	Amministratore dei sistemi di backup.	9. Autorizzato (almeno in lettura) all'accesso: 1. dei dump dei database (o direttamente delle istanze in caso di utilizzo di agent); 2. delle share di rete; 3. dei system state e degli snapshot delle macchine; 4. delle configurazioni (che necessitano di backup); 5. degli export di specifici servizi; 6. dei log di tutte le macchine della rete.

Local Administrator & Technical Support	1	Amministratore di un dispositivo client (postazione di lavoro).	10. Autorizzato: 1. all'accesso completo ad un insieme specificato nella nomina di sistemi client ed ai dati contenuti nei dispositivi di memorizzazione (a meno di diversa ed esplicita configurazione); 2. all'analisi e controllo dei log locali.