Comune di Nola
Provincia di Napoli

Regolamento di gestione utenti e profili di autorizzazione per trattamenti elettronici

Sommario

Adottato con Delibera di G.M. n. 202 del 12/05/2011

Articolo I. Scopo

Il presente regolamento, con riferimento alle prescrizioni dettate dal D.Lgs 196/2003 (Disciplinare Tecnico - Allegato B) ed al vigente Documento Programmatico sulla Sicurezza, ha lo scopo di definire ruoli, responsabilità e necessità di protocolli operativi relativi alla gestione degli utenti delle infrastrutture informatiche in uso presso il Comune di Nola, con particolare riferimento ad una corretta gestione delle credenziali di autenticazione e del sistema di autorizzazione.

Esso si applica alla gestione delle piattaforme applicative (sistemi applicativi e sistemi di supporto) e dell'infrastruttura di rete (risorse ICT).

Articolo II. Riferimenti

Decreto Legislativo n. 196 del 2003 - Disciplinare Tecnico - Allegato B
Comune di Nola – Documento Programmatico sulla Sicurezza.
Garante Privacy - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008).

Articolo III. Definizioni e Glossario

Piattaforme Informatiche	Sono i sistemi ***software*** **e** ***hardware*** utilizzati dall'ente per la gestione delle attività istituzionali. Si tratta, tipicamente, di sistemi ***client/server***, che prevedono infrastrutture presso il Servizio SIC (Sistema Informativo Comunale) (***server*** **applicativi** e ***server*** **dati**) cui si collegano, tramite reti locali e geografiche, le postazioni *client* delle strutture organizzative utilizzatrici.
Applicazione	È sinonimo di programma. Si dice di qualsiasi software dedicato a un'attività specifica (videoscrittura, calcolo, gestione dati, giochi, etc).
Client	In generale è un computer collegato ad un server ma un client è anche il programma che, in un sistema client/server, inoltra le richieste dell'utente ad un programma server.
Hardware	Tutto ciò che in un sistema di elaborazione si riconosce fisicamente e quindi tutte le periferiche, le parti elettriche, meccaniche, elettroniche ed ottiche.
Rete	Termine generico che indica un insieme di mezzi fisici (computer, stampanti, apparati di comunicazione) connessi tra di loro allo scopo di condividere le risorse fisiche e il software nonchè consentire lo scambio di dati.
Rete Geografica - WAN	La rete che collega computer distribuiti su vaste aree geografiche (Wide area Network).
Rete Locale - LAN	Nel campo dell'informatica LAN è l'acronimo per il termine inglese Local Area Network, in italiano rete locale. Identifica una rete costituita da computer collegati tra loro

	(comprese le interconnessioni e le periferiche condivise) all'interno di un ambito fisico delimitato (ad esempio una stanza o un edificio, o anche più edifici vicini tra di loro) che non superi la distanza di qualche chilometro. Le LAN hanno dimensioni contenute, il che favorisce il tempo di trasmissione.
Server	Computer che utilizza un sistema operativo di rete e destinato a svolgere uno o più servizi quali ad esempio la gestione di una LAN, lo scambio e la condivisione di files (file server), la gestione della posta elettronica (mail server), l'ospitare sit web (web server), la gestione di periferiche come le stampanti (print server), il salvataggio (backup) dei dati. Le mansioni dei diversi tipi di server possono essere gestite da un solo computer o possono essere suddivise tra più macchine dedicate a ognuno dei servizi descritti. I computer ad esso collegati vengono definiti come client. Insieme costituiscono un sistema client/server.
Software	Software e' un termine generico che definisce programmi e procedure utilizzati per far eseguire al computer un determinato compito. Viene in generale suddiviso in: - software di base o di sistema, perchè è indispensabile al funzionamento del computer, dal momento che senza di esso non sarebbe che hardware inutilizzabile. Viene identificato con il sistema operativo; - software applicativo. Esso comprende i programmi che il programmatore realizza utilizzando le prestazioni che offre il sistema operativo; tra essi troviamo, ad esempio, applicazioni gestionali, destinati alle esigenze specifiche di un utente o di un'azienda e tutto ciò che riguarda l'automazione di ufficio.
Credenziali di autenticazione	Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. **Le credenziali di autenticazione** consistono in: un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato associato a un codice identificativo o a una parola chiave oppure una caratteristica biometrica (ad esempio impronta digitale) dell'incaricato associata a un codice identificativo o a una parola chiave.
Sistema di autorizzazione	Un sistema di autorizzazione è la modalità tecnica attraverso la quale si definisce, per un incaricato di trattamento elettronico dotato di credenziali di autenticazione, l'ambito di trattamento consentito dall'applicazione informatica. Il sistema di autorizzazione si stabilisce attraverso la definizione di profili di autorizzazione, ai quali possono

	essere associati gli incaricati o gruppi di essi. I profili di autorizzazione, per ciascun incaricato o per funzioni omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Attraverso un processo di autenticazione ed un connesso sistema di autorizzazione si consegue, in via generale, un accesso, da parte degli utenti, all'infrastruttura di rete ed ai connessi servizi erogati tramite sistemi hardware e software, come, ad esempio, un **file server**, che consente agli utenti di archiviare e condividere, su un'infrastruttura centralizzata, dati e informazioni, anche non gestiti tramite applicazioni client/server, organizzati in maniera tale da regolamentarne l'accesso e l'elaborazione secondo profili di autorizzazione e privilegi di accesso definiti.
Risorse ICT	Piattaforme Informatiche (Applicazioni); Infrastrutture di rete e connettività (sistemi e apparati); Postazioni di lavoro; Servizi di supporto: Posta elettronica, Archiviazioni condivise, Servizi ICT in genere.
Back-up e ripristino	Procedure mediante le quali si ottiene il salvataggio esterno di dati e configurazioni, al fine di garantirne il possibile recupero (ripristino) in caso di perdite dovute a malfunzionamenti o eventi disastrosi.

Articolo IV. Ruoli e Responsabilità

(a) Amministratore di Sistema (AS)

La funzione di Amministratore di Sistema (AS), con riferimento alle infrastrutture ICT in uso presso il Comune di Nola, è svolta dal **Servizio Informativo Comunale (SIC)**.

Il responsabile del servizio – **Responsabile dell'Amministrazione dei Sistemi** – individua gli eventuali ulteriori amministratori necessari (amministratori di sistema, amministratori di rete, amministratori applicativi, amministratori di database).

Il **Responsabile dell'Amministrazione dei Sistemi** e gli ulteriori **incaricati di funzioni amministrative** (amministratori di sistema, amministratori di rete, amministratori di database, amministratori applicativi), sono formalmente incaricati dal Titolare dei trattamenti, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato.

La designazione degli incaricati è individuale e, per ognuno, è indicata l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. L'elenco degli incaricati, con relativi funzioni e profili, è allegato al Documento Programmatico sulla Sicurezza.

Il SIC gestisce, salvo eccezione formalmente definite, le seguenti **risorse ICT**:

- Piattaforme Informatiche;
- Infrastrutture di rete e connettività (sistemi e apparati);
- Postazioni di lavoro;
- Servizi di supporto:
  - Posta elettronica;
  - Archiviazioni condivise;
  - Servizi ICT in genere.

Il **Responsabile dell'Amministrazione dei Sistemi** cura la gestione delle misure minime e adeguate per la protezione e sicurezza dei dati di cui alla vigente normativa e, in particolare:

- aggiorna annualmente, entro il mese di febbraio, l'inventario delle piattaforme informatiche utilizzate;
- tiene i rapporti con il Responsabili di Trattamento al fine di rilasciare abilitazioni, accessi e credenziali relativamente alle risorse ICT;
- aggiunge, rimuove, aggiorna e rilascia informazioni riguardanti le credenziali di autenticazione degli utenti (codice identificativo dell'utente + password, ecc.) e comunica agli incaricati, in maniera riservata, l'avvenuta abilitazione ai servizi richiesti e le relative credenziali di autenticazione, secondo quanto richiesto dai Responsabili di Trattamento;
- associa utenti e gruppi a profili di autorizzazione;
- attiva, disattiva, varia o sospende le abilitazioni degli utenti (ingresso, uscita, spostamento, prolungata inattività (6 mesi)) all'utilizzo dei servizi offerti dall'infrastruttura, secondo quanto richiesto dai Responsabili di Trattamento o, di propria iniziativa, per ragioni di sicurezza; in tale ultimo caso, dà comunicazione di tali attività al Titolare dei Trattamenti;
- comunica agli incaricati, in maniera riservata, l'avvenuta abilitazione ai servizi richiesti e le relative credenziali di autenticazione
- documenta la lista degli utenti (attivi, inattivi, sospesi, ecc.) e i relativi profili di autorizzazione;
- definisce e applica le politiche relative alle credenziali di autenticazione (uso della password, composizione, scadenza, ecc.), dandone informazione agli utenti;
- verifica annualmente, entro il mese di febbraio, insieme ai Responsabili di Trattamento, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, applica gli eventuali relativi aggiustamenti e custodisce il relativo verbale;
- esegue i salvataggi dei dati e delle configurazioni e custodisce in sicurezza i relativi supporti;

- esegue test periodici di ripristino di dati e configurazioni;
- ripristina dati e configurazioni nei tempi previsti dalla legge;
- assicura l'efficace applicazione, quando richiesto, di metodi di crittografia;
- installa, configura e manutiene sistemi hardware e software;
- esegue gli aggiornamenti dei sistemi operativi, *patches* e cambiamenti di configurazione;
- esegue audit sui sistemi e sul software applicativo;
- assicura la funzionalità dell'infrastruttura di rete;
- applica le politiche di sicurezza;
- analizza e risolve problemi di funzionamento e/o performance;
- tiene, in via esclusiva, i rapporti con outsourcers e software houses, definendo e controllando le modalità di accesso di tali enti esterni alle piattaforme informatiche, a fini di *service*, manutenzione ordinaria e straordinaria e per interventi occasionali;
- prepara e raccoglie le lettere di nomina a Responsabile esterno di trattamento elettronico, a firma del Titolare dei trattamenti;
- cura la comunicazione al personale, per il tramite del Titolare dei trattamenti, dei nominativi dei soggetti che, in virtù dell'incarico ad amministratore, possono accedere a servizi o sistemi che trattano, anche indirettamente, dati personali dei lavoratori;
- implementa sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e dello stesso responsabile. 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, non inferiore a sei mesi. Le registrazioni (access log), tenute secondo le prescrizioni del Garante per la protezione dei dati personali, sono messe a disposizione del Titolare dei trattamenti, che le utilizza a fini di verifica delle attività.

(b) Responsabile di trattamento (RT)

I Responsabili di Trattamento, nominati dal Titolare secondo quanto previsto nel Documento Programmatico sulla Sicurezza, definiscono formalmente gli incaricati di trattamento nell'ambito delle proprie aree di competenza. Coerentemente con tali definizioni, RT, sempre con riferimento agli incaricati della propria area di competenza, definisce le modalità di accesso degli incaricati alle risorse ICT, con particolare riferimento alle Piattaforme Informatiche e alle archiviazioni condivise.

Per queste categorie di risorse deve essere sempre garantita la coerenza tra l'ambito di trattamento consentito (indicato nelle lettere formali di incarico) e i concreti profili di autorizzazione o i privilegi di accesso alle risorse ICT.

Il Responsabile di Trattamento:

- è l'interfaccia unica con l'Amministratore di Sistema per quanto attiene alla gestione degli incaricati (credenziali di autenticazione e profili di autorizzazione);
- definisce, per le unità organizzative coinvolte nell'utilizzo delle risorse ICT, il modulo di indicazione degli incaricati e dei relativi profili di autorizzazione;
- comunica all'Amministratore di Sistema, utilizzando il *Modulo di richiesta servizi ICT,* i nominativi del personale incaricato di trattamento elettronico dei dati, i servizi richiesti, i connessi privilegi e i profili di autorizzazione;
- comunica all'Amministratore di Sistema, utilizzando il *Modulo di richiesta servizi ICT*, ogni evento significativo relativo al personale incaricato di trattamento elettronico:
    - ingresso utente nell'unità organizzativa,
    - uscita utente dall'unità organizzativa,
    - modifica di attribuzioni (variazione di profilo o di privilegi, sospensioni, revoche).
- verifica annualmente, entro il mese di febbraio, insieme all'Amministratore di Sistema, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Articolo V. Audit

Il Titolare di Trattamenti, nell'ambito delle attività di revisione periodica del Documento Programmatico sulla Sicurezza, così come previsto anche dalla norma, dispone un audit *indipendente* e specifico sul processo di gestione degli utenti delle piattaforme informatiche, orientato alla verifica del rispetto delle prescrizioni di legge e a quanto programmato nel DPS vigente.

Il Titolare di Trattamenti, inoltre, dispone, con cadenza annuale, secondo quanto indicato nel Provvedimento del Garante per la protezione dei dati personali del 27.1.2.2008, attività di verifica dell'operato degli amministratori di sistema, in particolare per quanto riguarda gli accessi.

Articolo VI. Documenti e moduli

Modulo richiesta servizi ICT

Comune di Nola
Provincia di Napoli
***S**ervizio **I**nformatica **C**omunale*

Data _____/____/_____ Prot. n°_____

Il Dirigente:_____ Ufficio _____

Nominativo dipendente_____

Chiede un intervento per:

□ Malfunzionamento/Disservizio □ Dominio/File server/risorse di rete □ Posta elettronica

□ Abilitazioni all'uso di sw applicativi □ Collaudo □ Altro

(descrizione sintetica richiesta)

_____

_____

Marca e modello/Ubicazione (se trattasi di apparecchiature):

_____

_____

_____

Disposizione attribuzioni: □inserimento □sospensione □revoca □variazione di profilo

_____

Firma_____

Riservato al SIC