

Allegato n. 3 – Procedura per la gestione delle abilitazioni di accesso al protocollo informatico

Approvato con determinazione dirigenziale n. 1699 del 22/06/2023
Aggiornato con determinazione dirigenziale n. 3316 del 16/12/2024

La presente procedura è finalizzata alla definizione del controllo degli accessi al sistema di gestione informatica dei documenti, da parte di utenti o gruppi di utenti, al fine di garantire la sicurezza del sistema, nonché la riservatezza delle informazioni e la protezione dei dati personali in esso contenuti, grazie al tracciamento degli eventi sulle informazioni trattate e all'individuazione dell'autore.

Il sistema di gestione documentale permette abilitazioni e profili di accesso differenziati in base alle tipologie di operazioni da compiere. Gli accessi sono rilasciati tenendo conto dei ruoli, delle funzioni e delle competenze dei soggetti da abilitare al sistema.

Il sistema di protocollo informatico in uso prevede la gestione dei seguenti permessi e profili:

Profilo/Ruolo	Descrizione
Protocollo_Visualizza	Gruppo utenze per la consultazione e visualizzazione del protocollo
Atti_Protocollo_Inserimento	Gruppo utenze per la consultazione, visualizzazione, stampa, smistamento e registrazione protocolli
Protocollo_Visualizza_Tutto	Gruppo utenze per la consultazione e visualizzazione dei protocolli anche appartenenti ad altri uffici
Atti_Protocollo_Gestione	Gruppo utenze per la consultazione, visualizzazione, gestione, stampa, registrazione, assegnazione, annullamento, smistamento del protocollo
Administrator	Gruppo utenze di amministratori dell'applicativo Sicra
Administrator demografici	Gruppo utenze di amministratori del Settore Servizi Demografici
Amministratori jiride	Gruppo utenze di amministratori dell'applicativo Jiride
Amministratori di sistema	Gruppo utenze di amministratori di sistema
Maggioli security token	Gruppo utenze della software house Maggioli
Ws_protocollo gestione	Gruppo utenze della software house Maggioli
Saga	Gruppo utenze della software house Maggioli
<u>Crea protocolli altri uffici</u>	<u>Gruppo utenze per la protocollazione per altri uffici</u>

I livelli di autorizzazione sono attribuiti dal Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO.

Le abilitazioni sono avallate dal Responsabile della gestione documentale o suo delegato su proposta del Dirigente/Responsabile di Posizione organizzativa del settore richiedente.



L'accesso al sistema da parte degli utenti avviene tramite: USER/PASSWORD

All'utente abilitato viene assegnata una credenziale pubblica che permette l'identificazione dell'utente da parte del sistema (user ID) e una componente riservata di autenticazione (password).

Gli utenti, così abilitati, accedono al sistema mediante le credenziali di accesso ricevute. Al primo accesso viene richiesto il cambio password secondo i criteri di complessità richiesti dal sistema. In nessun caso la password deve essere ceduta a terzi e dovrà essere modificata dal proprietario ogni 90 giorni.

Richiesta di creazione o modifica di un utente interno

Il Dirigente/Responsabile di posizione organizzativa, valutata la necessità di abilitare un utente o gruppi di utenti della UO di sua competenza al sistema di gestione informatica dei documenti, invia richiesta al Responsabile della gestione documentale o al suo delegato all'indirizzo di posta elettronica proto@comune.brescia.it.

La richiesta deve comprendere:

- dati identificativi dell'utente da abilitare;
- permessi e profili di accesso che è necessario associare all'utente.

Il Responsabile della gestione documentale o suo delegato valuta la richiesta e autorizza l'abilitazione degli utenti e la configurazione dei profili di accesso, inoltrando la richiesta ai tecnici dell'informatica su apposita casella dell'assistenza Sicra. Il Settore Transizione Digitale, acquisita l'autorizzazione del Responsabile della gestione documentale, provvede all'abilitazione degli utenti e alla configurazione dei profili di accesso.

All'utente abilitato è richiesta un'adeguata formazione all'utilizzo del sistema di gestione documentale.

In caso di trasferimento di un utente da una UO ad un'altra UO sarà cura del Dirigente/Responsabile di posizione organizzativa della UO di destinazione richiedere, come da procedura al paragrafo precedente, la modifica dei profili di accesso del nuovo utente.

Richiesta disabilitazione di un utente interno

Qualora un utente abilitato al sistema di gestione documentale cessi il rapporto di lavoro in essere è necessario che venga effettuata richiesta di disabilitazione.

Periodicamente il Settore Risorse umane comunica la cessazione dell'utente, chiedendo la disabilitazione dell'account.

La disattivazione dell'account viene richiesta al Settore Transizione Digitale dal Settore Risorse Umane in caso di cessazione di servizio oppure dal Responsabile del Settore in tutti gli altri casi.

Richiesta di abilitazione per utenti esterni

Il Dirigente/Responsabile di posizione organizzativa, valutata la necessità di abilitare un utente o gruppi di utenti esterni alla UO di sua competenza al sistema di gestione informatica dei documenti, invia una mail ai tecnici dell'Informatica su apposita casella dell'assistenza Sicra e al Settore Segreteria generale, prevenzione della corruzione e trasparenza, utilizzando l'apposito modulo a disposizione nella intranet comunale nel quale devono essere inseriti:

- dati identificativi dell'utente da abilitare;
- permessi e profili di accesso che è necessario associare all'utente;
- motivazione specifica per l'abilitazione (esempio: riferimento contrattuale, normativa).

Il Settore Transizione Digitale, acquisita l'autorizzazione del Responsabile della gestione documentale, provvede all'abilitazione degli utenti e alla configurazione dei profili di accesso.



Richiesta disabilitazione di un utente esterno

Nel momento in cui l'accesso da parte di utenti esterni non è più necessario si deve procedere alla disabilitazione dell'utenza.

Il Dirigente/Responsabile di posizione organizzativa comunica la cessazione dell'utente chiedendo la disabilitazione dell'account al Settore Transizione Digitale e al Settore Segreteria generale, prevenzione della corruzione e trasparenza.