COMUNE DI ANCONA
Servizio Sistemi Informativi

Procedura Operativa per la gestione degli accessi al Sistema Informativo Comunale

Codice Versione:	001
Data emissione:	38562
Distribuzione:	Personale del Comune di Ancona e autorizzati all'accesso alla rete informatica

INDICE GENERALE

1. PREMESSA

La regolamentazione degli accessi al sistema informativo comunale è un passo fondamentale per ridurre i rischi di accesso di persone non autorizzate ai dati gestiti dal Comune.

Il Documento programmatico della sicurezza del Comune di Ancona approvato con delibera di giunta n. 828 del 30/12/2005 all'art. *10 – Misure di sicurezza* stabilisce che solo gli incaricati dotati di appropriate credenziali accedono al sistema informativo del Comune e solo dopo il superamento di una procedura di autenticazione. Lo stesso articolo definisce che le credenziali di autenticazione consistono in un codice univoco (Account) composto da un nome utente (Username) ed una parola chiave riservata e conosciuta solamente dal medesimo (Password).

Il Regolamento relativo all'accesso e all'uso delle rete informatica e telematica del Comune di Ancona approvato con delibera di giunta n. 823 del 29/12/2005 all'art. *8 - Modalità di accesso alla rete e ai servizi/programmi per gli utenti interni* specifica che le modalità di uso e gestione degli Account sono definite con apposita Procedura Operativa.

2. SCOPO

Con la presente Procedura Operativa il Comune di Ancona intende regolamentare la gestione dell'accesso ai dati, per proteggere il proprio patrimonio informativo, per garantire la continuità dei servizi erogati a favore della cittadinanza e dell'utenza esterna in generale e per assicurare il pieno rispetto della normativa vigente in tema di protezione dei dati personali (Dlgs 30/6/2003 n. 196).

In particolare vengono descritte:

a) le modalità di richiesta degli Account sia per gli utenti Interni sia per gli Esterni
b) le modalità di creazione degli Account
c) le modalità di comunicazione degli Account agli interessati
d) il riesame dei diritti di accesso e relativa comunicazione agli interessati
e) le modalità di creazione e gestione delle password.

3. RIFERIMENTI

Decreto Legislativo 196 del 30 Giugno 2003
Documento programmatico della sicurezza del Comune di Ancona (delibera di giunta n. 828 del 30/12/2005)
Regolamento relativo all'accesso e all'uso delle rete informatica e telematica del Comune di Ancona (delibera di giunta n. 823 del 29/12/2005)

4. ALLEGATI

MOD-SSI-001-A-Richiesta accesso e uso della rete informatica
MOD-SSI-001-B-Richiesta accesso ai servizi-programmi
MOD-SSI-001-C-Autorizzazione accessi
MOD-SSI-001-D-Comunicazione accessi autorizzati
MOD-SSI-001-E-Comunicazione accessi non autorizzati
MOD-SSI-001-F-Richiesta riesame diritti di accesso
MOD-SSI-001-G-Autorizzazione riesame diritti di accesso
MOD-SSI-001-H-Comunicazione riesame diritti di accesso

MOD-SSI-001-AE-Richiesta accesso sistema informativo per utenti esterni
MOD-SSI-001-BE-Richiesta accesso alle banche dati per utenti esterni
MOD-SSI-001-FE-Richiesta revoca diritti di accesso per utenti esterni

5. CAMPO DI APPLICAZIONE

A tutti gli utenti Interni del Comune di Ancona e a tutti gli utenti Esterni che utilizzano il sistema informativo comunale.

6. LISTA DI DISTRIBUZIONE

Questo documento è reso disponibile per gli utenti Interni nella Intranet comunale e per gli utenti Esterni sul sito del Comune di Ancona.

7. RESPONSABILITA'

Dirigente del Servizio Personale	Ha la responsabilità di richiedere al Dirigente del Servizio Sistemi Informativi la creazione degli Account di rete e posta elettronica per ogni neoassunto; ha inoltre il compito di richiedere il riesame dei diritti di accesso per i dipendenti che cessano il rapporto di lavoro o cambiano servizio di appartenenza.
Dirigenti dei Servizi	Sono responsabili del trattamento dei dati di competenza e degli accessi autorizzati agli stessi, relativamente ai dipendenti del servizio. Hanno inoltre la responsabilità di autorizzare le richieste di accesso alle banche dati di competenza inoltrate da altri Dirigenti dei Servizi o da Enti esterni.
Dirigente del Servizio Sistemi Informativi	Ha la responsabilità di autorizzare e disporre la creazione dei

	nuovi account ed il riesame dei diritti di accesso.
Amministratore di rete e referenti tecnici	Hanno la responsabilità della creazione, cancellazione, modifica degli account e assegnazione delle password temporanee. Hanno inoltre la responsabilità delle comunicazioni all'utente finale previste dalla presente Procedura Operativa.
Utenti Interni ed Esterni	Hanno la responsabilità di gestire le loro password nella modalità descritta in questa Procedura Operativa e di utilizzare il sistema informativo comunale nei limiti degli accessi autorizzati.

8. MODALITA' ESECUTIVE

8.1. RICHIESTA ACCOUNT DI RETE, DI POSTA ELETTRONICA E DEGLI APPLICATIVI PER UTENTI INTERNI

Per poter accedere ed usare le risorse informatiche ed i relativi servizi, ogni utente Interno deve utilizzare i propri Account.

Per quanto riguarda gli Account di rete e di posta elettronica, la richiesta deve essere presentata al Servizio Sistemi Informativi e sottoscritta dal Dirigente del Servizio Personale.

Tale richiesta (**MOD-SSI-001-A-Richiesta accesso e uso della rete informatica**) deve indicare:

- data richiesta
- nominativo del Dirigente che sottoscrive
- cognome e nome dell'utente Interno
- servizio di appartenenza
- data di assunzione ed eventualmente data di scadenza del contratto
- matricola dell'utente.

Per quanto riguarda gli Account applicativi, la richiesta deve essere presentata al Servizio Sistemi Informativi e sottoscritta dal Dirigente del Servizio di appartenenza. Nel caso in cui l'utente abbia necessità di accedere a banche dati di cui il Dirigente non è direttamente responsabile, la richiesta deve essere sottoscritta anche dal Dirigente Responsabile del trattamento dei dati.

Tale richiesta (**MOD-SSI-001-B-Richiesta accesso ai servizi-programmi**) deve indicare:

- data richiesta
- nominativo del Dirigente del Servizio di appartenenza
- servizio di appartenenza
- cognome e nome dell'utente Interno
- servizi/programmi per i quali l'utente deve essere autorizzato.

8.2. RICHIESTA ACCESSO AL SISTEMA INFORMATIVO PER GLI UTENTI ESTERNI

Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che gli utenti Esterni sottoscrivano con il Comune di Ancona apposita convenzione e che presentino al Servizio Sistemi Informativi il modello **MOD-SSI-001-AE-Richiesta accesso sistema informativo per utenti esterni**.

La richiesta deve essere sottoscritta dal Responsabile dell'Ente/Azienda e deve indicare:

- data richiesta
- nominativo del Responsabile dell'Ente/Azienda
- denominazione dell'Ente/Azienda richiedente
- scopo per il quale si richiede l'accesso al sistema informativo comunale
- cognome e nome dell'incaricato autorizzato all'accesso
- luogo e data di nascita
- codice fiscale
- numero di telefono dell'ufficio
- eventuale e-mail
- firma per accettazione al trattamento dei dati personali per la generazione degli identificativi di accesso ed al trattamento dei file di registrazione di tutte le attività di collegamento e di visura di dati, ai sensi di quanto stabilito dal D.Lgs. n. 196/2003.

Nel caso in cui venga richiesto l'accesso ad una banca dati, il Dirigente del Servizio Sistemi Informativi deve richiedere l'autorizzazione all'accesso al Dirigente Responsabile del trattamento dei dati, utilizzando il modello **MOD-SSI-001-BE-Richiesta accesso alle banche dati per utenti esterni**.

8.3. CREAZIONE DEGLI ACCOUNT

Il Dirigente del Servizio Sistemi Informativi esamina le richieste di accesso, controlla che le stesse siano debitamente compilate e sottoscritte, provvede a trasmetterle al personale competente unitamente al modello **MOD-SSI-001-C-Autorizzazione accessi**, con il quale autorizza la creazione degli account.

8.3.1. CREAZIONE DEGLI ACCOUNT DI RETE E DI POSTA ELETTRONICA

Gli Account di rete e di posta elettronica vengono generati dall'Amministratore di rete con la seguente modalità:

Il nome utente per accesso alla rete informatica viene composto prendendo le prime tre lettere del cognome ed aggiungendo le prime tre lettere del nome. Nei casi di omonimia l'ultima lettera viene cambiata per ottenere un nome utente univoco.
L'indirizzo di posta elettronica viene generato nella modalità nome.cognome@comune.ancona.it.

Per gli Utenti Interni tutti gli Account hanno le seguenti caratteristiche:
Il nome utente ha la lunghezza di n. 6 caratteri e viene composto come descritto al punto precedente.

Per gli Utenti Esterni tutti gli Account hanno le seguenti caratteristiche:
Il nome utente è costituito da una descrizione breve del'ente con aggiunto un numero progressivo di due cifre

Gli Amministratori di rete hanno Account specifici e personali per svolgere il lavoro di amministrazione e gestione della rete e dei server.

8.3.2. CREAZIONE DEGLI ACCOUNT APPLICATIVI

Gli Account applicativi vengono generati dai referenti tecnici degli applicativi con la seguente modalità:

1) Il Codice Personale (Username) è generato seguendo la stessa modalità sopradescritta per la creazione dell'utente di rete.
2) Viene generata dal referente tecnico una Parola chiave (Password) temporanea con scadenza immediata, in modo che l'utente sia costretto a cambiare tale Password al primo accesso.
3) Se l'utente ha un contratto a termine, verrà impostato un periodo di validità dell'Account, in modo che venga automaticamente disabilitato dall'applicativo al termine del periodo stabilito.

Ad ogni Account vengono assegnate le funzionalità applicative, cioè le abilitazioni concesse nell'utilizzo del servizio/programma.

Per quanto riguarda gli utenti Interni, si attribuiscono tali funzionalità in base a quanto indicato nelle abilitazioni specifiche al servizio/programma del modulo di richiesta (**MOD-SSI-001-B-Richiesta accesso ai servizi-programmi**). In assenza di tali informazioni, il referente tecnico assegna le funzionalità applicative tenendo conto dell'attività lavorativa svolta dall'utente nel servizio di appartenenza e le specifica nel modello **MOD-SSI-001-C-Autorizzazione accessi**.

Per quanto riguarda gli utenti Esterni, si attribuiscono tali funzionalità in base a quanto indicato nella convenzione con l'Ente/Azienda ed a quanto specificato nello scopo della richiesta di accesso al sistema informativo (**MOD-SSI-001-AE-Richiesta accesso sistema informativo per utenti esterni**).

I referenti tecnici hanno Account specifici e personali per svolgere il lavoro di amministrazione e gestione degli applicativi.

Gli account che non vengono utilizzati per un periodo superiore ai mesi 6 (sei), verranno disattivati.

8.4. COMUNICAZIONE DEGLI ACCESSI AL RICHIEDENTE

Gli utenti Interni devono recarsi personalmente presso gli uffici del Servizio Sistemi Informativi per ritirare la comunicazione degli accessi, sia quelli autorizzati (**MOD-SSI-001-D-Comunicazione accessi autorizzati**), sia quelli non autorizzati (**MOD-SSI-001-E-Comunicazione accessi non autorizzati**). Gli Account vengono consegnati in busta chiusa e sigillata e l'utente deve apporre la data e la firma sul modello **MOD-SSI-001-C-Autorizzazione accessi** per presa in consegna degli Account.

Per gli utenti Esterni è possibile ritirare la comunicazione degli accessi personalmente presso gli uffici del Servizio Sistemi Informativi oppure ricevere la stessa tramite raccomandata. Nel primo caso il richiedente è tenuto ad apporre la data e la firma sul modello **MOD-SSI-001-C-Autorizzazione accessi** per presa in consegna degli Account.

8.5. RIESAME DEI DIRITTI DI ACCESSO

Nel caso di cessazione del rapporto di lavoro o di spostamento dell'utente Interno in altro servizio, il Dirigente del Servizio Personale deve darne comunicazione al Servizio Sistemi Informativi utilizzando il modello **MOD-SSI-001-F-Richiesta riesame diritti di accesso**. Il Dirigente del Servizio Sistemi Informativi esamina le richieste e provvede a trasmetterle al personale competente unitamente al modello **MOD-SSI-001-G-Autorizzazione riesame diritti accesso**, con il quale autorizza il riesame dei diritti di accesso.

Per gli utenti Esterni, se vengono a mancare, per la persona incaricata, i requisiti per l'autorizzazione all'accesso, l'Ente/Azienda è tenuta a richiedere tempestivamente al Servizio Sistemi Informativi la revoca dei diritti di accesso, utilizzando il modello **MOD-SSI-001-FE-Richiesta revoca diritti accesso**

per utenti esterni. Il Dirigente del Servizio Sistemi Informativi esamina le richieste e provvede a trasmetterle al personale competente unitamente al modello **MOD-SSI-001-G-Autorizzazione riesame diritti accesso**, con il quale autorizza il riesame dei diritti di accesso.

8.6. COMUNICAZIONE DEL RIESAME DEI DIRITTI DI ACCESSO

Gli utenti Interni devono recarsi personalmente presso gli uffici del Servizio Sistemi Informativi per ritirare la comunicazione del riesame dei diritti di accesso (MOD-SSI-001-H-Comunicazione riesame diritti accesso). Detta comunicazione viene consegnata in busta chiusa e sigillata e l'utente deve apporre la data e la firma sul modello **MOD-SSI-001-G-Autorizzazione riesame diritti accesso** per presa in consegna della comunicazione.

Per gli utenti Esterni è possibile ritirare la comunicazione del riesame degli accessi personalmente presso gli uffici del Servizio Sistemi Informativi oppure ricevere la stessa tramite raccomandata. Nel primo caso il richiedente è tenuto ad apporre la data e la firma sul modello **MOD-SSI-001-G-Autorizzazione riesame diritti accesso** per presa in consegna della comunicazione.

8.7. GENERAZIONE E GESTIONE DELLE PASSWORD

Le password sono una componente fondamentale degli Account, poiché forniscono un mezzo per l'autenticazione degli utenti. E' determinante, quindi, per la sicurezza del sistema informativo, che le password siano di qualità.

8.7.1. CRITERI PER GENERARE PASSWORD DI QUALITA'

Le password per essere definite di qualità vanno generate secondo regole che garantiscano un buon livello di sicurezza.

Le password devono avere una lunghezza minima di otto caratteri, e devono possibilmente essere facili da ricordare, in modo da evitare eventuali trascrizioni.

Le password non devono presentare una sequenza di caratteri identici (es. AAAAAAAA, 55555555, ecc.), e non devono essere formate da gruppi di caratteri tutti numerici o tutti alfabetici (es. AAAA1111, AA11BB22, ecc.). È raccomandato l'uso di caratteri maiuscoli, minuscoli, numeri e caratteri speciali.

Le password non devono essere basate su nomi di persone, animali, oggetti, o comunque ricavabili da un dizionario, anche di lingua straniera.
E' molto importante che la scelta degli utenti non ricada mai su parole deducibili da informazioni personali o dei propri familiari (come nome e cognome, numeri telefonici, date di nascita, codice fiscale, ecc…).

Si indicano di seguito alcuni suggerimenti per fare in modo che la password selezionata risponda al criterio di complessità e sia facilmente memorizzabile.

Si potrebbe, ad esempio, scegliere una frase facilmente memorizzabile e si potrebbero utilizzare come password le iniziali di ciascuna parola di cui è composta la frase, sostituendo alcuni caratteri con numeri e con caratteri speciali.
Ad esempio la frase "Io abito in Via Milano 4 a Ancona" potrebbe diventare IAIVM4AA.
Si potrebbero poi alternare lettere minuscole a lettere maiuscole, ottenendo la password iAiVm4Aa.
Per rispondere al criterio di complessità previsto dal sistema operativo di rete, si può sostituire alle "i" dell'esempio il numero "1" e sostituire alla "a" finale un carattere speciale, nell'esempio 1A1Vm4A@.

Allo stesso modo potrebbero essere usate frasi di fantasia o testi di canzoni, utilizzando solo le iniziali, in modo che la password sia un insieme di caratteri di senso non compiuto ma semplice da memorizzare, in quanto costituita dalle iniziali di una frase che conosciamo bene. Ad esempio "Nel Mezzo Del Cammin Di Nostra Vita" potrebbe diventare NMDCDNV, e usando maiuscole e minuscole diventerebbe NmDcDnV. Si potrebbe poi usare un carattere speciale: NmDcDn% e due numeri: Nm0c0n%.

Ogni utente potrebbe avere necessità di gestire diversi accessi con password. Ad esempio, l'accesso alla rete del Comune, l'accesso al programma del protocollo, l'accesso al programma della contabilità, ecc.
Tutte le password di accesso devono essere generate come indicato dalla presente procedura.

8.7.2. GESTIONE DELLE PASSWORD

Il Servizio Sistemi Informativi assegna ad ogni nuovo Account una password temporanea, che deve essere valida solo per un accesso. La password temporanea non deve avere una lunghezza inferiore a otto caratteri e deve essere possibilmente univoca.

L'utente al primo collegamento deve necessariamente cambiare la password assegnatagli con un'altra scelta da lui, che rispetti le caratteristiche indicate al paragrafo 8.1 di questa procedura operativa "Criteri per generare password di qualità".

L'utente dovrebbe evitare di trascrivere la password su carta, a meno che non sia possibile custodirla in modo sicuro (i criteri di sicurezza da usare sono gli stessi con cui si custodirebbe il codice PIN di una carta di credito o di un bancomat). La password non deve mai essere memorizzata in un processo automatico di log-in, ad esempio in una macro o in un tasto funzionale.

Se l'utente dimentica la password, dovrà rivolgersi al Servizio Sistemi Informativi per richiedere l'assegnazione di una nuova password temporanea.

Nel caso all'utente si presentasse una qualsiasi indicazione che una delle sue password non sia più sicura in quanto conosciuta da altre persone, deve immediatamente

- richiedere una nuova password temporanea al Servizio Sistemi Informativi (nel caso non possa direttamente cambiarla lui);
- modificare la sua password (nel caso possa farlo lui direttamente);

Tutti gli utenti devono sapere che le password scelte da loro, avranno validità di 3 (tre) mesi, a partire dalla loro creazione. Dopo questo periodo saranno obbligati a sostituirle con altre nuove, sempre basate sulle regole trattate in questa procedura. La password inserita ha una validità minima di un giorno, ossia non è possibile sostituirla due volte nello stesso giorno.

L'utente non deve reiterare le password già usate, in quanto il sistema memorizza le ultime quattro password utilizzate.

Il personale del Servizio Sistemi Informativi deve modificare le password associate agli username con privilegi di amministrazione con una periodicità almeno mensile.

E' essenziale che gli utenti mantengano le password confidenziali per motivi di sicurezza e per tutela degli utenti stessi. Il software di rete infatti memorizza le attività che vengono effettuate dai singoli utenti. Queste informazioni non vengono normalmente controllate dall'Amministratore di Sistema o suoi delegati per motivi di privacy, ma possono essere utilizzate nel caso in cui si verifichino incidenti o nel caso in cui si accertino attività illecite. Il sistema ovviamente non è in grado di distinguere se un utente connesso tramite ID e password è davvero la persona titolare di quell'account o se si tratta di un'altra persona che utilizza un account non suo. Non concedere la

propria password ad un'altra persona è quindi un sistema di tutela, per evitare che siano addebitate azioni che non sono state fatte.

I dati relativi ai propri Account non devono mai essere portati a conoscenza del personale esterno al Comune (consulenti, dipendenti di altri enti o aziende, ecc.). Gli utenti Esterni possono accedere al sistema informativo del Comune, anche solo temporaneamente, nella modalità di cui al paragrafo 3 della presente procedura.