



| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |




Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL

Linea Guida per la creazione e gestione degli utenti

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

Indice

| | | |
|-------|---|---|
| 1 | Introduzione | 3 |
| 2 | Obblighi degli utenti | 4 |
| 2.1 | Regole per la costruzione della password | 4 |
| 2.2 | Utilizzo e Conservazione della Password | 5 |
| 2.2.1 | Regole di riservatezza delle password | 5 |
| 2.2.2 | Primo accesso..... | 5 |
| 2.2.3 | Utilizzo e Conservazione | 6 |
| 2.3 | Scadenza della password | 6 |
| 2.4 | Sostituzione della password | 6 |
| 3 | Obblighi degli amministratori delle utenze..... | 7 |
| 4 | Responsabilità della DCOD INAIL | 7 |
| 4.1 | Predisposizione di un sistema di log | 7 |
| 4.2 | Monitoraggio..... | 8 |
| 4.3 | Accesso ai dati dei file di log | 8 |
| 4.4 | Periodo di Conservazione e Cancellazione dei file di log..... | 8 |

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

1 Introduzione

Sulla base degli accordi tra INAIL e Ministero del Lavoro e delle Politiche Sociali, gli utenti del Ministero possono accedere ai seguenti servizi:

| |
|--|
| Consultazione Libro Unico |
| Anagrafica Ditte non Inail (Libro Unico) |
| Dichiarazione RLS (Rappresentante dei Lavoratori per la Sicurezza) |
| Dichiarazione Unità produttive |
| Consultazione Anagrafica Ditta |
| Sportello DURC |
| Gestione Diffide art. 16 |
| Diffide 2° grado |
| Gestione DTL |
| Sanzioni amministrative – Rapporto DTL art. 17 L.689/1981 |


Per consentire al Ministero di gestire direttamente i propri utenti e le relative abilitazioni, l'INAIL ha realizzato il servizio "Gestione Utenti e Profili".

Tramite questo servizio, l'amministratore centrale del Ministero, indicato da quest'ultimo e abilitato da INAIL, può creare e gestire le utenze per il proprio personale.

A INAIL spetta il compito di creare l'utenza dell'amministratore centrale e di comunicare all'assegnatario la relativa password provvisoria di primo accesso.

Gli utenti del Ministero del Lavoro possono accedere ai servizi, collegandosi al portale www.inail.it e autenticandosi utilizzando come credenziali il proprio codice fiscale e la password. In alternativa gli utenti possono utilizzare la CNS (Carta nazionale dei servizi) cliccando sul bottone "SmartCard".

Per consultare la base dati DURC, gli utenti "Ispettori del lavoro" devono collegarsi a www.sportellounicoprevidenziale.it e autenticarsi utilizzando come credenziali il

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

proprio codice fiscale e la password.

2 Obblighi degli utenti

Ogni utente è responsabile della corretta gestione delle credenziali di accesso e, in particolare, è tenuto a salvaguardare la segretezza della password, come previsto dal D.Lgs. 196/03 per gli incaricati del trattamento dei dati personali e precisato anche nel presente documento.


La password personale è uno strumento che tutela sia l'INAIL, sia l'utente da eventuali accessi illeciti da parte di persone non autorizzate ai servizi e alle informazioni. La sua corretta scelta, seguita da una gestione mirata a preservarne la riservatezza, è il modo migliore per garantire la tutela dei dati personali prevista dalla legge.

A tale scopo nei paragrafi successivi sono indicate le regole da seguire per la costruzione, l'utilizzo e la gestione della password.

2.1 Regole per la costruzione della password

Il sistema di autenticazione obbliga l'utente a modificare direttamente la password al primo accesso e a modificarla obbligatoriamente almeno ogni 90 giorni. Per la costruzione e gestione della password, l'utente deve attenersi alle seguenti regole:

- La lunghezza della password deve essere di almeno 8 caratteri;
- La password può essere costruita utilizzando caratteri numerici, alfabetici, lettere maiuscole o minuscole e segni di interpunzione;
- Le password devono contenere almeno un carattere numerico;
- Occorre evitare l'utilizzo di termini facilmente riconducibili al titolare della password stessa (per esempio nome, cognome, data di nascita, nome dei familiari, date di ricorrenze personali, sigle aziendali di Funzioni

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

Organizzative e progetti, la propria user-id di accesso ad altri sistemi informatici, la matricola);

- Occorre altresì evitare l'utilizzo di termini di uso eccessivamente comune o facili da ricordare (per esempio nomi di personaggi famosi, nomi dei mesi, dei giorni della settimana, delle stagioni, degli Stati, delle città).

2.2 Utilizzo e Conservazione della Password

2.2.1 Regole di riservatezza delle password

È necessario adottare un comportamento di riservatezza per le credenziali di accesso al portale INAIL e in particolare non è consentito:

- Comunicare le credenziali di autenticazione (codice identificativo e password) o condividerle con altre persone;
- Consentire a terzi l'accesso al servizio con le proprie credenziali utente;
- Accedere al servizio utilizzando le credenziali di un altro utente.


In caso di accesso illecito ai dati personali contenuti nelle banche dati dell'INAIL da parte di terzi; il titolare dell'utenza risponde della violazione delle leggi vigenti.

2.2.2 Primo accesso

Al primo accesso, a ogni utente è richiesta la registrazione, mediante l'inserimento dei propri dati anagrafici. Tra i dati anagrafici previsti, ai fini della sicurezza, è particolarmente importante l'indicazione della propria casella di posta elettronica, perché permette di richiedere e ricevere una nuova password nel caso in cui l'utente l'abbia dimenticata.

Al termine della registrazione, l'utente è tenuto a cambiare la password provvisoria iniziale.

In caso di variazione dei dati anagrafici (es. numero di telefono, indirizzo, posta

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

elettronica, ecc.), gli utenti sono tenuti ad aggiornarli, cliccando sul pulsante "Profilo" e selezionando nel menù a sinistra "Modifica Anagrafica".

2.2.3 Utilizzo e Conservazione

La password deve essere custodita dal titolare con la massima accuratezza, in modo tale da impedire a chiunque di venirci a conoscenza. In particolare è importante non scrivere la password su fogli, biglietti facilmente rinvenibili o comunque conservati in posti non sicuri.

Inoltre, occorre prestare attenzione a non lasciare incustodita la propria postazione di lavoro dopo aver aperto una sessione di lavoro.

2.3 Scadenza della password

La password ha un periodo massimo di validità di 90 giorni passati i quali l'utente deve modificarla. L'utente può comunque effettuare il cambio della password in qualunque momento senza attendere la scadenza.


Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate¹.

2.4 Sostituzione della password

L'utente deve provvedere alla sostituzione della password cliccando sul pulsante "Profilo" e selezionando nel menù a sinistra "Cambia Password", se è stata comunicata ad altri o si sospetta un'eventuale compromissione della segretezza.

Nel caso in cui la password sia stata dimenticata, l'utente può richiedere una nuova password cliccando su "password dimenticata?", nell'home page di www.inail.it e la nuova password sarà inviata alla casella di posta indicata nella scheda anagrafica.

¹ Cifrato regola 7 dell'Disciplinare Tecnico in materia di misure minime di sicurezza, allegato B al D.LGS 196/03

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

3 Obblighi degli amministratori delle utenze

Gli amministratori delle utenze sono tenuti a verificare periodicamente, con cadenza almeno annuale, la sussistenza delle esigenze che hanno portato all'attivazione delle utenze abilitate all'accesso ai servizi². In caso di cambio di mansioni, trasferimento pensionamento o qualsiasi altro evento che implichi il venir meno della legittimazione a consultazione i dati messi a disposizione dall'INAIL, l'amministratore deve provvedere a disattivare l'utenza.

Gli amministratori devono archiviare la documentazione relativa alle verifiche periodiche svolte, in particolare le liste di utenze con i rispettivi profili aggiornate, anche per poterle esibire in caso di eventuali controlli.

4 Responsabilità della DCOD INAIL


La DCOD è responsabile degli aspetti di sicurezza tecnico-organizzativi inerenti il servizio. Definisce le procedure organizzative e/o operative che regolamentano il servizio e controlla il rispetto delle regole generali ivi espresse.

4.1 Predisposizione di un sistema di log

Al fine di consentire verifiche e controlli sull'utilizzo dell'applicazione e poter individuare le responsabilità di eventuali attività illecite, la DCOD deve provvedere alla registrazione, in un sistema di archiviazione sicuro, delle attività degli utenti, in conformità con i vincoli normativi e legislativi vigenti (si vedano, per esempio, il D.Lgs. 196/2003, il Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e Internet", il 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").

Tali registrazioni sono conservate inizialmente sui sistemi di esercizio e,

² Cifrato regola 8 del Disciplinare Tecnico in materia di misure minime di sicurezza, allegato B al D.LGS 196/03: "le credenziali devono essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali"

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

successivamente, archiviate per un periodo di tempo coerente con la tipologia di dati trattati e nel rispetto dei vincoli legislativi.

Inoltre, per garantire il rispetto dei requisiti di riservatezza, integrità e disponibilità, devono essere adottate opportune misure di sicurezza per i sistemi preposti alla conservazione dei dati di log.

In conformità con le indicazioni del Provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008, sono tracciate anche le attività di gestione delle utenze, per permettere controlli sull'operato degli amministratori e poter identificare eventuali abusi o attività illecite.

4.2 Monitoraggio

La DCOD svolge attività di controllo e monitoraggio dell'operato dei diversi soggetti coinvolti, effettua controlli periodici sui log dei sistemi di autenticazione per la verifica degli accessi. Il monitoraggio deve avvenire soltanto al fine esclusivo di difesa del patrimonio informativo dell'Istituto, per prevenire e rilevare tempestivamente usi illeciti o abusi dei servizi accessibili dal portale di INAIL. Pertanto, i log delle attività degli utenti che accedono ai servizi sono trattati ai soli fini dei controlli difensivi, secondo le disposizioni di legge.


4.3 Accesso ai dati dei file di log

Al personale INAIL preposto alla gestione del servizio e dei log, non è consentito l'accesso ai dati se non a fronte di particolari eventi di sicurezza. È consentita l'analisi dei report, in forma aggregata e anonima, per l'individuazione delle possibili contromisure idonee a risolvere eventuali problemi di sicurezza.

L'utilizzo dei dati raccolti, quindi, può avvenire esclusivamente per le finalità di analisi statistiche o per rilevare, per esempio, l'uso non autorizzato, frodi o attacchi informatici e sempre nel rispetto della legislazione sulla privacy in vigore.

4.4 Periodo di Conservazione e Cancellazione dei file di log

Le registrazioni devono essere conservate per un periodo di tempo coerente con la tipologia di dati trattati e nel rispetto dei vincoli legislativi.

| | | | |
|---|--|--|---|
|  | | <i>Tipo documento:</i> Linea Guida | |
| <i>Emesso da:</i> DCOD | <i>Titolo Documento:</i> <i>Accesso degli utenti del Ministero del Lavoro e delle Politiche Sociali ai servizi INAIL</i> <i>Linea Guida per la creazione e gestione degli utenti</i> | <i>Versione</i> 1.2 | <i>Data di emissione</i> 14-04-2015 |

In conformità con il Provvedimento del Garante del 1 marzo 2007, la configurazione dei sistemi informatici deve prevedere la cancellazione periodica ed automatica dei file di log contenenti dati personali relativi agli accessi al servizio, la cui conservazione non sia necessaria, conservandoli per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza. L'eliminazione dei dati allo scadere del periodo di conservazione deve essere effettuata con particolare attenzione: devono essere cancellati o resi anonimi, eliminandoli anche dalle copie di back-up create per il salvataggio dei dati, in modo da rendere i dati irrecuperabili anche successivamente.

Nello specifico, l'Istituto conserva i log per un periodo minimo di 6 mesi, fino ad un massimo di 2 anni.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- Ad esigenze tecniche o di sicurezza del tutto particolari;
- All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire le finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.