GENERALITÀ

Le misure di sicurezza per la gestione dei documenti informatici conservati sull'applicativo di protocollo informatico riguardano, tra altro, anche l'assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione.

Il cambio delle password avviene con frequenza al massimo *trimestrale* durante la fase di esercizio.

I dati personali o le user ID di accesso di cui sopra, registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzati saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto, dalle FF.OO ed Autorità giudiziarie.

Le credenziali di accesso al sistema sono del tutto personali e il loro uso ricade sotto la responsabilità di ciascun utente cui sono assegnate. Il personale abilitato è tenuto alla diligente custodia delle credenziali che ai sensi dell'art. 1 co. 1 lett. p del CAD sono assimilabili ad una firma elettronica e quindi incedibili.

Per accedere al sistema ogni utente deve disporre di:

- **PROFILO:** autorizzazioni concesse dal responsabile del servizio;
- **USER_ID:** identifica l'utente mediante i dati personali, (solitamente C.F.);
- **PASSWORD:** stringa segreta e riservata all'utente che, in combinazione con il ruolo, consente di accedere al sistema. Essa è associata allo *user_id.*

Resta inteso che ogni persona fisica può ricoprire più ruoli mantenendo comunque, la stessa *password* di accesso legata, quest'ultima, al proprio *user_id.*

Il controllo degli accessi è pertanto, assicurato utilizzando le credenziali di accesso e un sistema di autorizzazione basato sulla profilatura degli utenti in via preventiva.

Le regole per la composizione delle password sono le seguenti:

- essere composta da almeno un carattere maiuscolo, uno minuscolo, uno speciale ed uno numerico
- avere lunghezza minima di 6 caratteri
- ammettere i caratteri speciali elencati in parentesi: (/*-+,.:;)
- risultare case sensitive (i caratteri maiuscoli sono percepiti DIVERSI dagli analoghi minuscoli. Es.: M diverso da m)
- essere diversa dalle 6 password precedenti

Non è consentito cedere a terzi le credenziali personali di accesso alla propria postazione di lavoro, alla posta elettronica ed agli applicativi di gestione dei flussi documentali. Eventuali eccezioni vanno segnalate ed opportunamente formalizzate, informando sempre gl'interessati.

Firmato digitalmente da FILISETTI MARCO UGO
ND: c=IT, o=MINISTERO ISTRUZIONE UNIVERSITA' E RICERCA/80185250588, cn=FILISETTI MARCO UGO, serialNumber=IT:FLSMCG68B07A794A, givenName=MARCO UGO, sn=FILISETTI, dnQualifier=3588568
Data: 2015.10.09 16:41:59 +02'00'