IRPET Istituto Regionale Programmazione Economica della Toscana

DISCIPLINARE INTERNO SULLA GESTIONE DELLE CREDENZIALI

(approvato con determinazione n. del)

Indice generale

1. 1. INTRODUZIONE

L'Ente mette a disposizione del proprio personale e di eventuali collaboratori esterni i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- strumenti di informatica individuale, quali personal computer e relativi accessori, scanner ecc.
- apparati e servizi condivisi, quali ad esempio, posta elettronica, internet, stampanti di rete sistemi di condivisione file, server, apparati di rete ecc.
- programmi di produttività individuale e procedure gestionali
- Applicativi specialistici per elaborazioni statistiche, programmazione e gestione banche dati.

Tali risorse costituiscono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.

Le pubbliche amministrazioni sono tenute ad assicurare il corretto impiego degli strumenti ICT e della telefonia da parte dei propri operatori, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa. Questo avviene nell'ottica di garantire la sicurezza, la disponibilità e l'integrità dei sistemi e di prevenire sprechi. Esiste quindi in capo agli operatori l'obbligo, sancito da norme di legge e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa, e questo anche nell'utilizzo delle risorse aziendali. In particolare l'art. 11 comma 3 del Codice di comportamento dei dipendenti dell'Ente prevede che "*Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione*". Tale prescrizione riguarda quindi anche l'uso delle risorse informatiche, nell'utilizzo delle quali il dipendente deve agire in modo da non pregiudicare e ostacolare le attività dell'Ente o perseguire interessi privati in contrasto con quelli pubblici.
Viene quindi posto l'obbligo, in carico ai dirigenti, di vigilanza sul corretto utilizzo degli strumenti di lavoro e di prevenzione per garantire la migliore sicurezza e disponibilità delle proprie strutture e risorse, tra cui in primis i dati utilizzati e amministrati.

Il corretto utilizzo da parte degli utenti di queste risorse del sistema informatico dell'Ente è disciplinato nel documento 'DISCIPLINARE INTERNO SULL'USO DI INTERNET, POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI'.

In capo a coloro che svolgono le funzioni di Amministratore di Sistema, sia in qualità di dipendenti dell'Ente, sia in veste di responsabili (ai sensi del Regolamento 2016/679 del Parlamento Europeo), così come individuati dalle disposizioni de Disposizioni dell'Autorità Garante per la protezione dei dati personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"*, ricade la responsabilità aggiuntiva di una corretta gestione delle credenziali di accesso ai vari costituenti il sistema informatico dell'Ente improntata ai principi di professionalità, proporzionalità e verificabilità.

Il corretto funzionamento del sistema, la disponibilità e l'affidabilità delle risorse che rendono possibile l'attività istituzionale dell'Ente non possono prescindere dalle misure di sicurezza adottate e poste in essere. Tali misure sono declinate secondo diversi approcci e ambiti, di cui il comportamento individuale del personale dell'Ente di cui sopra è solo uno, seppure fondamentale. Altri ambiti altrettanto importanti riguardano le misure a garanzia della sicurezza e continuità fisica del servizio (ridondanza fisica e logica degli apparati, gruppi di continuità elettrici, sistemi anti-incendio e anti-intrusione, ecc.), la politica di backup dei dati e dei sistemi, i sistemi di log e di monitoraggio, la politica di protezione dei dati e infine la politica di gestione delle credenziali e degli accessi.

Il presente documento disciplina i criteri e i comportamenti cui gli amministratori di sistema devono attenersi nella gestione del ciclo di vita delle credenziali di accesso ai vari sistemi e risorse messe a

disposizione dall'Ente, demandando a specifici documenti la disciplina e le norme relative a tutti gli altri aspetti e dimensioni della sicurezza.

Questo documento illustra quindi le norme generali di attribuzione, gestione e distruzione delle credenziali di accesso alle risorse informatiche che il Servizio Informatico e gli Amministratori di Sistema in generale devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Ente nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei propri sistemi informativi. Questo documento fornisce inoltre un ulteriore necessario apporto nella costruzione di una struttura aziendale coerente e conforme ai dettami del Regolamento 2016/679 sulla protezione dei dati personali. La sua osservanza garantisce inoltre una maggiore coerenza e imparzialità nel trattamento degli utenti.

2. CAMPO DI APPLICAZIONE

Le regole descritte nel presente documento devono essere rispettate da tutti gli iscritti nel registro degli amministratori di sistema (inclusi i consulenti esterni), indipendentemente dal tipo di incarico svolto e dalla sede dell'attività.
La gestione delle risorse strumentali, ivi incluse quelle informatiche, compete ai Dirigenti, che si assumono le responsabilità legate al corretto utilizzo ed all'osservanza delle norme.

3. NORMATIVA DI RIFERIMENTO

Il presente Disciplinare Interno è redatto in conformità alla normativa alla normativa vigente, di seguito riportata per riferimento:

- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori).

- Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

- Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

- Decreto Legislativo 30 giugno 2003, n°. 196 "Codice in materia di protezione dei dati personali", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure fisiche, logiche e organizzative che devono essere adottate al fine di: evitare possibili distruzioni, perdite, alterazioni di dati; garantire che l'accesso ai dati sia effettuato dalle sole persone

incaricate al trattamento e quindi autorizzate; garantire che il trattamento avvenga per le finalità e nelle modalità consentite.

•Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)".

•Disciplinare interno sull'uso di internet, posta elettronica e altri strumenti informatici (in via di approvazione) che recepisce le misure minime di sicurezza ICT AGID, circolare n. 2/2018.

•Le misure di sicurezza sono applicate garantendo il rispetto di quanto disposto dalle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007.

•Raccomandazioni del Cert-PA di AgID per la sicurezza dello smart working 17 marzo 2020.

•Disposizioni dell'Autorità Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" e ss.mm.

•Disciplinare interno per Amministratori di Sistema

4. CREDENZIALI E ACCESSI ALLE POSTAZIONI DI LAVORO

a. Principi generali

Le credenziali (nome utente e password) per l'accesso ai servizi informatici dell'Ente vengono rilasciate dal Servizio Informatico previa richiesta da parte del dirigente cui fa capo l'interessato. Il personale del servizio provvede inoltre a rigenerare password scadute o dimenticate ed a disattivare le utenze cessate. L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi e alle risorse dell'Ente, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, uso improprio della propria posta elettronica etc.).

Le postazioni di lavoro fisse dell'Ente con sistema operativo Windows sono inserite in un dominio Microsoft Active Desktop e gli utenti del dominio sono gestiti in maniera centralizzata dall'amministratore del dominio (Servizio informatico o Amministratore di sistema), non hanno privilegi di amministratore.
I notebook con sistema operativo Windows utilizzati anche fuori sede e per connessioni in VPN richiedono necessariamente che l'utente abbia privilegi di amministratore, così come certe applicazioni specifiche anche su pc fissi in sede, per cui si ammette in via eccezionale l'attribuzione di credenziali con privilegi di amministratore, sempre e solo limitatamente alla singola macchina. Questo stato di necessità altamente indesiderabile comporta l'introduzione di vulnerabilità nella sicurezza del sistema informatico in generale e deve essere rimosso non appena soluzioni tecniche hardware/software lo consentano.
Altre postazioni di lavoro sia fisse che notebook sono equipaggiate con sistema operativo Linux. In considerazione della diversa natura del sistema e delle vulnerabilità cui è soggetto, oltre alle necessità già descritte per le postazioni di lavoro utilizzate fuori sede, anche per queste si ammette l'attribuzione di credenziali con privilegi puntuali di amministratore (comando sudo). Questa disposizione può essere rivista in considerazione dell'evolversi della situazione e delle minacce.

E' fatto tassativo divieto di collegare alla rete locale dell'Ente risorse informatiche private (notebook, tablet, smartphone, periferiche etc.), salvo preventiva ed esplicita autorizzazione del personale del Servizio Informatico previa richiesta scritta e motivata da parte del dirigente cui fa capo l'interessato; in caso di autorizzazione, l'utente è tenuto a rispettare le configurazioni di sistema disposte dal Servizio Informatico ed il rispetto delle misure minime di sicurezza descritte nell'allegato B del D.Lgs 196/2003 e ss.mm.

Per i dispositivi considerati non affidabili è messa a disposizione la connessione wifi 'irpet-ospiti' che abilita l'accesso a internet mantenendo il dispositivo isolato dalle risorse della rete locale.

b. Creazione

La creazione di credenziali per l'accesso al dominio o alle singole postazioni di lavoro dell'Ente è competenza del Servizio Informatico e di quanti sono registrati nel registro degli amministratori di sistema.

La creazione delle credenziali deve seguire le seguenti disposizioni:

- Le credenziali per l'accesso alle postazioni di lavoro per gli utenti ordinari devono essere nominali e personali; è fatto divieto di attribuire a un utente le credenziali create per un utente diverso. E' altresì assolutamente vietato la condivisione delle proprie credenziali di accesso con altri.
- Le utenze ordinarie delle postazioni di lavoro non devono avere privilegi di amministratore, salvo quando questa condizione sia un impedimento oggettivo all'utilizzo delle funzionalità e dei programmi richiesti dall'attività dell'utente.
- Le credenziali per utenze di amministrazione/gestione generiche e di default (es.: root, administrator, ecc.) devono essere utilizzate nei limiti del possibile solo nella fase iniziale di configurazione e di generazione di ulteriori credenziali di amministratore personali e nominali.
- Al primo accesso gli utenti possono/devono modificare la password preimpostata ricevuta con una che devono aver cura di mantenere segreta.
- Per gli utenti ordinari di dominio la politica di sicurezza del dominio deve imporre il rinnovo periodico della password e un controllo delle specifiche di solidità e sicurezza. La complessità e la frequenza di sostituzione della password devono aderire alle specifiche riportate in appendice A al presente documento.
- Le eventuali credenziali di accesso a file system criptato o a BIOS impostate esclusivamente dall'amministratore di sistema devono essere registrate in un apposito documento contenente l'elenco delle postazioni di lavoro, insieme alle altre informazioni relative alla postazione di lavoro, quali caratteristiche tecniche, numero seriale, numero di inventario, MAC address, utente assegnatario. L'elenco deve essere conservato in modo idoneo a garantirne la riservatezza e la disponibilità agli amministratori di sistema e al Servizio Informatico.

Le credenziali di accesso alle postazioni di lavoro devono essere trasmessi in modalità sicura, ovvero direttamente o tramite applicazioni di comunicazione ritenute ragionevolmente sicure, quale a esempio Signal che utilizza un canale interamente criptato; per la trasmissione di credenziali è vietato l'utilizzo di sistemi o programmi di dubbia affidabilità (al momento della stesura di questo documento sono da ritenersi tali la posta elettronica, il telefono, le piattaforme di comunicazione sociale, messaggistica e teleconferenza quali twitter, whatsapp, skype, zoom). Qualora fosse ineludibile l'utilizzo di canali di trasmissione non sicuri le informazioni devono essere trasmesse utilizzando più canali in modo che su ciascuno di essi l'informazione sia incompleta.

Per i requisiti delle password degli utenti e le corrette modalità di uso e conservazione si rimanda al documento 'DISCIPLINARE INTERNO SULL'USO DI INTERNET, POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI' in via di approvazione.

c. Utilizzo

L'amministratore di sistema può richiedere all'utente la password per interventi di assistenza e risoluzione di problemi. Al termine dell'intervento l'utente deve modificare la propria password.

d. Chiusura

Alla cessazione dell'attività lavorativa presso l'Ente di un dipendente titolare di credenziali di accesso a una postazione di lavoro, il dirigente cui fa capo deve darne comunicazione scritta al Servizio Informatico affinché proceda alla chiusura delle utenze correlate.
In occasione della sostituzione di una macchina o dell'assegnazione di una nuova postazione a un utente, le utenze sulla macchina dismessa o sostituita devono essere tempestivamente rimosse.

5. CREDENZIALI E ACCESSI AI SERVER

a. Principi generali

Le credenziali di accesso ai server dell'Ente sono gestite in autonomia dal Servizio Informatico e di quanti sono registrati nel registro degli amministratori di sistema.
Nel registro degli amministratori di sistema devono essere riportate espressamente le competenze di ciascuno in relazione ai server e ai servizi gestiti.

b. Creazione

La creazione di credenziali per l'accesso ai server dell'Ente è competenza del Servizio Informatico e di quanti sono registrati nel registro degli amministratori di sistema.
La creazione delle credenziali deve seguire le seguenti disposizioni:

- Le utenze di amministrazione/gestione generiche e di default (es.: root, administrator, ecc.) devono essere utilizzate nei limiti del possibile solo nella fase iniziale di configurazione e di generazione di ulteriori credenziali di amministratore personali e nominali.
- Le credenziali di amministratore personali e nominali devono essere rinnovate secondo le modalità e le tempistiche riportate nella tabella in in appendice A al presente documento; è fatto divieto di attribuire a un utente le credenziali create per un utente diverso. E' altresì assolutamente vietato la condivisione delle proprie credenziali di accesso con altri.
- Le eventuali credenziali di accesso a file system criptato o a BIOS impostate esclusivamente dall'amministratore di sistema devono essere registrate in un apposito documento contenente l'elenco dei server, insieme alle altre informazioni relative alla macchina, quali caratteristiche tecniche, numero seriale, numero di inventario, MAC address. L'elenco deve essere conservato in modo idoneo a garantirne la riservatezza e la disponibilità agli amministratori di sistema e al Servizio Informatico.

Le credenziali di accesso a server/servizi devono essere trasmessi in modalità sicura, ovvero direttamente o tramite applicazioni di comunicazione ritenute ragionevolmente sicure, quale a esempio Signal che utilizza un canale interamente criptato; per la trasmissione di credenziali è vietato l'utilizzo di sistemi o programmi di dubbia affidabilità (al momento della stesura di questo documento sono da ritenersi tali la posta elettronica, il telefono, le piattaforme di comunicazione sociale, messaggistica e teleconferenza quali twitter, whatsapp, skype, zoom). Qualora fosse ineludibile l'utilizzo di canali di trasmissione non sicuri le informazioni devono essere trasmesse utilizzando più canali in modo che su ciascuno di essi l'informazione sia incompleta.

c. Utilizzo

E' sempre opportuno prevedere un rinnovo periodico delle credenziali di amministrazione dei server e servizi sulla base della tempistica indicata nella tabella di appendice A, obbligatorio nel caso di sistemi gestiti in proprio.
Nel caso di sistemi gestiti o co-gestiti da fornitori esterni si impone estrema cautela onde evitare disservizi e problemi.
Per loro natura tali server ospitano servizi installati e gestiti da fornitori esterni che per funzionare correttamente (almeno in alcune specifiche fasi) richiedono l'utilizzo delle credenziali di amministratore.
E' pertanto necessario prima di procedere a un cambiamento delle password di amministrazione verificare la sussistenza di tali dipendenze e procedere a contattare la ditta che fornisce la manutenzione del servizio e concordare con essa la modifica.

d. Chiusura

Alla cessazione dell'esigenza che ha determinato la messa in esercizio di un server / servizio o in caso di sostituzione dell'hardware il sistema va distrutto ovvero reso disponibile per nuove attività mediante formattazione.

6. CREDENZIALI E ACCESSI A BANCHE DATI

a. Principi generali

L'Ente dispone di banche dati su piattaforma mysql ospitate su server locali o dislocati presso SCT, alcune delle quali contenenti dati personali. L'attività degli amministratori di sistema deve essere improntata a garantire per quanto possibile la sicurezza e l'integrità dei dati e la tranciabilità delle operazioni che su essi vengono svolte. A tal fine essi provvedono ad abilitare l'accesso ai dati e la loro manipolazione agli autorizzati limitatamente alle esigenze della propria attività e al periodico rinnovo delle credenziali di accesso.

b. Creazione

La creazione di credenziali per l'accesso a banche dati dell'Ente è competenza del Servizio Informatico e di quanti sono registrati nel registro degli amministratori di sistema.
La creazione delle credenziali deve seguire le seguenti disposizioni:

- Le credenziali per le banche dati per gli utenti ordinari devono essere nominali e personali; è fatto divieto di attribuire a un utente le credenziali create per un utente diverso. E' altresì assolutamente vietato la condivisione delle proprie credenziali di accesso con altri.
- Le credenziali per utenze di amministrazione/gestione generiche e di default (es.: root, sysadmin, ecc.) devono essere utilizzate nei limiti del possibile solo nella fase iniziale di configurazione e di generazione di ulteriori credenziali di amministratore personali e nominali.
- Le credenziali per utenti ordinari e per amministratori/gestori devono contemplare i privilegi strettamente necessari all'espletamento delle attività per cui l'utenza viene creata.
- La complessità e la frequenza di sostituzione della password devono aderire alle specifiche riportate in appendice A al presente documento.

Dove non fosse possibile per limitazioni tecnologiche applicare questi criteri è obbligo attenersi alle opzioni più stringenti consentite dal sistema. In tali situazioni l'amministratore della banca dati è tenuto fornire al dirigente del servizio informatico una valutazione sul problema e possibili soluzioni o interventi mitigatori.

Le credenziali di accesso alla banca dati devono essere trasmessi in modalità sicura, ovvero direttamente o tramite applicazioni di comunicazione ritenute ragionevolmente sicure, quale a esempio Signal che utilizza un canale interamente criptato; per la trasmissione di credenziali è vietato l'utilizzo di sistemi o programmi di dubbia affidabilità (al momento della stesura di questo documento sono da ritenersi tali la posta elettronica, il telefono, le piattaforme di comunicazione sociale, messaggistica e teleconferenza quali twitter, whatsapp, skype, zoom). Qualora fosse ineludibile l'utilizzo di canali di trasmissione non sicuri le informazioni devono essere trasmesse utilizzando più canali in modo che su ciascuno di essi l'informazione sia incompleta.

c. Utilizzo

L'amministratore di sistema deve tenere un elenco sempre aggiornato delle utenze e il loro stato, che deve riportare le seguenti informazioni:

- titolare
- tipologia (amministratore, ordinario, ecc.)
- username
- password
- data creazione
- data ultima modifica della password

•data di chiusura programmata (se prevista) o effettiva

L'elenco deve essere conservato in modo idoneo a garantirne la riservatezza e la disponibilità.
Sulla base della tempistica indicata nella tabella di appendice A deve provvedere al periodico rinnovo della password e a una ricognizione sull'utilizzo delle utenze, provvedendo a chiudere quelle la cui esistenza non è più giustificata.

d. Chiusura

Alla cessazione dell'attività lavorativa presso l'Ente di un dipendente titolare di credenziali di accesso a una banca dati o nell'eventualità di un suo cambiamento di ruolo o di funzioni, il dirigente cui fa capo deve darne comunicazione scritta al Servizio Informatico affinché proceda alla chiusura delle utenze correlate.
Il servizio Informatico o l'amministratore di sistema che ha preso in carico la segnalazione provvede ad aggiornare la lista delle utenze segnalando la data di chiusura.

7. CASELLA DI POSTA ELETTRONICA

a. Principi generali

L'Ente fornisce un servizio di posta elettronica, mettendo a disposizione indirizzi con dominio @irpet.it; gli indirizzi possono essere individuali o per servizio, questi ultimi vengono richiesti dal responsabile dello stesso e condivisi tra più lavoratori. Il servizio di posta elettronica è uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali. Il data base di posta è di esclusiva proprietà dell'Ente, il personale del Servizio Informatico per motivi tecnici e di sicurezza, in particolare per prevenire o correggere malfunzionamenti, può accedere al suo contenuto nel rispetto della normativa vigente.
Per un corretto utilizzo della posta elettronica dell'Ente si rimanda al documento 'DISCIPLINARE INTERNO SULL'USO DI INTERNET, POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI'.

b. Creazione

Le caselle di posta del dominio @irpet.it possono essere di natura nominale e personale oppure istituzionale non nominale.
La creazione di una nuova casella di posta elettronica con dominio @irpet.it è realizzata dal Servizio Informatico dietro istanza scritta (anche semplicemente una e-mail) del dirigente interessato.
Le caselle di posta nominali/personali possono essere assegnate esclusivamente al personale dell'Ente con rapporto di lavoro subordinato a tempo indeterminato o determinato o titolari di specifica borsa di studio presso Irpet. Non hanno quindi diritto alla casella nominale/personale a esempio stagisti, visitatori, collaboratori occasionali, ex dipendenti.
Per l'apertura di una casella di posta nominale/personale il titolare dovrà fornire al Servizio informatico tutte le informazioni personali richieste dalla procedura: luogo e data di nascita, codice fiscale, recapito telefonico o e-mail alternativo (opzionale).
Per le caselle istituzionali/non nominali verranno generati codici fiscali e dati anagrafici fittizi.
Al titolare o gestore della casella di posta verranno forniti i codici Pin e PUK generati automaticamente dalla procedura, trasmessi in modalità sicura, ovvero direttamente o tramite applicazioni di comunicazione ritenute ragionevolmente sicure, quale a esempio Signal che utilizza un canale interamente criptato; per la trasmissione di credenziali è vietato l'utilizzo di sistemi o programmi di dubbia affidabilità (al momento della stesura di questo documento sono da ritenersi tali la posta elettronica stessa, il telefono, le piattaforme di comunicazione sociale, messaggistica e teleconferenza quali twitter, whatsapp, skype, zoom). Qualora fosse ineludibile l'utilizzo di canali di trasmissione non sicuri le informazioni devono essere trasmesse utilizzando più canali in modo che su ciascuno di essi l'informazione sia incompleta.

c. Utilizzo

Per l'uso del servizio di posta elettronica, si richiede di osservare le seguenti norme comportamentali:

- L'uso della posta elettronica aziendale è consentito esclusivamente per motivi attinenti allo svolgimento delle mansioni assegnate, l'utente del servizio è consapevole che i contenuti della posta elettronica dell'Ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa;
- il Servizio Informatico fornisce assistenza all'uso ed alla configurazione esclusivamente per i programmi client autorizzati su dispositivi di proprietà dell'Ente;
- il titolare della casella è consapevole che il personale del servizio informatico nello svolgimento sua attività di assistenza tecnica e risoluzione di problemi inerenti il servizio di posta elettronica può prendere visione – seppure involontariamente – dei contenuti delle mail contenute nella casella.
- Il gestore di una casella di posta elettronica istituzionale / non nominale è consapevole che il contenuto di quella casella è accessibile a tutti coloro che siano abilitati.
- Nel caso il titolare richieda il reinoltro delle credenziali o l'impostazione di nuove, le modalità di trasmissione dovranno seguire gli stessi criteri definiti sopra per la creazione.

d. Cessazione

Alla cessazione dell'attività lavorativa presso l'Ente del dipendente/borsista o quando venga meno la ragione d'essere di una casella di posta istituzionale/non nominale, su indicazione del dirigente responsabile del titolare della casella e/o del Servizio Amministrazione, il Servizio Informatico provvederà a comunicare all'interessato la prossima chiusura della propria casella di posta – che deve avvenire l'ultimo giorno di servizio - , invitandolo al salvataggio di eventuali contenuti di interesse e fornendo assistenza nell'operazione, se richiesto.

La casella di posta elettronica del dipendente sarà chiusa (disattivata e resa irraggiungibile e immodificabile) e successivamente ne verrà richiesta la definitiva eliminazione al gestore del servizio di posta elettronica (fornitore individuato attraverso adesione a convenzione regionale).

8. USO DELLA RETE LOCALE, INTERNET E RISORSE CONDIVISE

a. Principi generali

Di norma ogni postazione di lavoro è connessa alla rete locale dell'Ente e agli utenti sono fornite le credenziali per l'accesso alla intranet, ad internet ed alle risorse di rete condivise funzionali all'attività lavorativa. Tali accessi devono avvenire esclusivamente per finalità istituzionali, strettamente connesse agli incarichi lavorativi svolti e sempre nel rispetto delle regole elencate nel documento 'DISCIPLINARE INTERNO SULL'USO DI INTERNET, POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI' in via di approvazione.

Ai dipendenti dell'Ente viene inoltre fornita ove necessario la possibilità di collegarsi in maniera sicura alle risorse e ai servizi interni dell'Ente via internet tramite l'utilizzo di VPN.

Credenziali per la connessione in VPN vengono inoltre concessi a collaboratori e fornitori che abbiano contratti in essere con l'Ente per la fornitura di servizi e prestazioni che richiedono attività da svolgere all'interno della rete locale dell'Ente.

Le credenziali (nome utente e password) per l'accesso alla rete wifi uffici, al servizio di condivisione in cloud dell'Ente e per la connessione in VPN alla rete interna dell'Ente vengono rilasciate dal Servizio Informatico previa richiesta da parte del dirigente cui fa capo l'interessato. Il personale del servizio provvede inoltre a disattivare le utenze cessate. L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi e alle risorse dell'Ente, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, etc.).

b. La rete wifi

L'ente dispone di due connessioni di rete wifi che abilitano l'accesso a risorse diverse: una rete 'ospiti' e una rete 'uffici'. Le credenziali per queste connessioni non sono personali/nominali, ma comuni e condivise.
Con la rete ospiti si ha l'accesso alla rete esterna, quindi è possibile navigare in internet e usufruire dei servizi che questa offre: le credenziali per questa connessione possono essere offerte a ospiti e visitatori per fornire loro un accesso a internet e possono essere utilizzate dal personale dell'Ente per la connessione di dispositivi personali, non di proprietà e sotto il controllo dell'Ente (per esempio notebook, tablet, smartphone personali dei dipendenti e/o visitatori/collaboratori esterni).
La rete 'uffici' dà l'accesso alle risorse interne della rete locale dell'Ente, quali condivisioni, stampanti, servizi in rete, e può essere utilizzata esclusivamente da dispositivi di proprietà dell'IRPET che hanno installato il software anti-malware adottato dall'Ente e regolarmente aggiornato. La password di accesso a tale rete deve essere distribuita esclusivamente al personale dipendente dell'ente o al personale appositamente autorizzato dal Dirigente responsabile del servizio informatico.
L'utilizzo di una password comune unica è giustificato dal fatto che l'accesso alla rete 'uffici' è comunque vincolato dall'indirizzo MAC del dispositivo che deve essere stato preventivamente registrato e abilitato dal Servizio informatico.
Il servizio informatico provvede alla registrazione di tutti i dispositivi di proprietà dell'Ente e del relativo MAC Address al momento della presa in carico delle macchine a ogni nuova fornitura.

c. Il servizio di cloud aziendale

La creazione di credenziali per l'accesso al cloud dell'Ente è competenza del Servizio Informatico e di quanti sono registrati nel registro degli amministratori di sistema, così come l'attribuzione di spazio disco sul server. E' realizzata dal Servizio Informatico dietro istanza scritta (anche semplicemente una e-mail) del dirigente interessato. La creazione delle credenziali deve seguire le seguenti disposizioni:

- Le credenziali per l'accesso al cloud aziendale per gli utenti ordinari devono essere nominali e personali; è fatto divieto di attribuire a un utente le credenziali create per un utente diverso. E' altresì assolutamente vietato la condivisione delle proprie credenziali di accesso con altri.
- Possono essere attivate utenze istituzionali generiche / non nominali su richiesta scritta del dirigente interessato. Tali utenze sono finalizzate alla gestione di progetti di lavoro di gruppo e le relative credenziali rimangono nell'esclusiva disponibilità del Servizio Informatico.
- L'attuale versione del sistema di cloud adottato non consente ai singoli utenti di modificare la propria password, pertanto essi dovranno utilizzare le credenziali fornite loro dal Sistema Informatico
- La complessità e la frequenza di sostituzione della password devono aderire alle specifiche riportate in appendice A al presente documento.

Le credenziali di accesso al cloud devono essere trasmessi in modalità sicura, ovvero direttamente o tramite applicazioni di comunicazione ritenute ragionevolmente sicure, quale a esempio Signal che utilizza un canale interamente criptato; per la trasmissione di credenziali è vietato l'utilizzo di sistemi o programmi di dubbia affidabilità (al momento della stesura di questo documento sono da ritenersi tali la posta elettronica, il telefono, le piattaforme di comunicazione sociale, messaggistica e teleconferenza quali twitter, whatsapp, skype, zoom). Qualora fosse ineludibile l'utilizzo di canali di trasmissione non sicuri le informazioni devono essere trasmesse utilizzando più canali in modo che su ciascuno di essi l'informazione sia incompleta.

d. VPN

L'ente mette una connessione VPN a disposizione dei propri dipendenti che hanno necessità di raggiungere risorse informatiche e servizi nella rete locale dell'Ente da una rete esterna.
Possono altresì usufruire della VPN aziendale anche soggetti esterni autorizzati dalla dirigenza.

Le credenziali di connessione VPN possono essere di natura nominale e personale oppure istituzionale non nominale.
La creazione di una nuova utenza VPN è realizzata dal Servizio Informatico dietro istanza scritta (anche semplicemente una e-mail) del dirigente interessato.

Le credenziali di accesso alla VPN non sono modificabili dall'utente.

Le credenziali di accesso alla VPN dell'Ente devono essere trasmessi in modalità sicura, ovvero direttamente o tramite applicazioni di comunicazione ritenute ragionevolmente sicure, quale a esempio Signal che utilizza un canale interamente criptato; per la trasmissione di credenziali è vietato l'utilizzo di sistemi o programmi di dubbia affidabilità (al momento della stesura di questo documento sono da ritenersi tali la posta elettronica, il telefono, le piattaforme di comunicazione sociale, messaggistica e teleconferenza quali twitter, whatsapp, skype, zoom). Qualora fosse ineludibile l'utilizzo di canali di trasmissione non sicuri le informazioni devono essere trasmesse utilizzando più canali in modo che su ciascuno di essi l'informazione sia incompleta.

L'amministratore di sistema deve tenere un elenco sempre aggiornato delle utenze e il loro stato, che deve riportare le seguenti informazioni:

- titolare
- ditta di appartenenza (se diversa dall'Ente)
- username
- password
- data creazione
- data ultima modifica della password
- data di chiusura programmata (se prevista) o effettiva

L'elenco deve essere conservato in modo idoneo a garantirne la riservatezza e la disponibilità.
Sulla base della tempistica indicata nella tabella di appendice A deve provvedere al periodico rinnovo della password e a una ricognizione sull'utilizzo delle utenze, provvedendo a chiudere quelle la cui esistenza non è più giustificata.

Alla cessazione del rapporto di lavoro o di servizio presso l'Ente di un titolare di credenziali di accesso VPN, il dirigente cui fa capo deve darne comunicazione scritta al Servizio Informatico affinché proceda alla chiusura delle utenze correlate.
In occasione della sostituzione di una macchina o dell'assegnazione di una nuova postazione a un utente, la configurazione VPN eventualmente presente sulla macchina dismessa o sostituita devono essere tempestivamente rimosse.

e. Apparati di rete

L'infrastruttura di rete dell'Ente è costituita, fra l'altro, da due switch di centro stella, uno switch di piano per ciascuna area fisica della sede e un certo numero di router wifi.
Tutti questi dispositivi devono essere ad accesso limitato e controllato, sia fisicamente (locali o armadi chiusi a chiave), sia tramite credenziali di opportuna solidità che devono rimanere nella esclusiva disponibilità del Servizio Informatico.
Nel caso dei router wifi, data l'impossibilità di limitarne l'accesso tramite chiusura a chiave è richiesto che vengano collocati in posizione elevata fuori portata.
È vietata l'installazione non autorizzata dal Servizio Informatico di propri dispositivi di connessione come Access Point, Router, Printer server, modem etc alla rete dell'Ente.

f. Gestionali e servizi esterni on-line

Per l'espletamento della propria attività istituzionale soprattutto in ambito amministrativo l'ente si avvale di servizi esterni on-line e di software gestionali le cui credenziali di accesso sono fornite direttamente ai singoli utenti in fase di registrazione (servizi on-line) o create dal fornitore (gestionale) e il cui ciclo di vita (attribuzione, manutenzione, chiusura) è al di fuori del controllo del Servizio Informatico. Il ruolo del Servizio Informatico in tale ambito si limita al fornire raccomandazioni di buone pratiche agli interessati.

9. FURTO O SMARRIMENTO

In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, il titolare è tenuto a informare tempestivamente il Servizio Informatico comunicando quali dati erano contenuti all'interno. Il Servizio Informatico provvederà immediatamente a una valutazione dei possibili rischi derivanti per eventuali personali, quindi se necessario comunicherà l'episodio al Security IT Manager e lo iscriverà nel registro degli incidenti di sicurezza conformemente alle disposizioni del Regolamento 2016/679 del Parlamento Europeo sulla protezione dei dati personali. Il Servizio Informatico provvederà inoltre immediatamente alla disabilitazione delle credenziali di VPN e di ogni altra credenziale compromessa.

10. CESSAZIONE DEL RAPPORTO DI LAVORO

Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Ente tutte le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per i Servizi.
La fase di cessazione prevede le seguenti modalità operative:

- Le credenziali fornite all'utente verranno disabilitate: è cura del responsabile del Servizio interessato comunicare le cessazioni degli utenti al Servizio Informatico;

- la casella di posta elettronica individuale verrà disattivata e successivamente cancellata: le attività necessarie per il passaggio delle consegne e la copia del materiale di interesse dell'Ufficio dovranno essere effettuati prima della disattivazione, a cura del responsabile del Servizio interessato; l'utente avrà a disposizione una settimana, salvo diversi accordi col Servizio Informatico, per la copia e salvataggio del contenuto della casella di posta elettronica a partire dalla data di cessazione del rapporto;

- le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio e legate alla casella di posta elettronica del dipendente, dovranno essere portate a conoscenza del Dirigente in tempo utile per consentire una loro migrazione verso altri utenti, ovvero la loro disabilitazione.

- le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore dell'Ente restano nella piena ed esclusiva disponibilità dell'Ente. L'utente non può formare, ottenere copia e/o cancellare documenti ed informazioni di interesse dell'Ente presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro a meno di esplicita autorizzazione scritta preventiva da parte del responsabile della struttura di appartenenza;

- le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per l'Ente verranno cancellate al termine del rapporto di lavoro senza alcuna responsabilità per l'Ente;

11. CONTROLLI

Disposizioni dell'Autorità Garante per la protezione dei dati personali ***"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"***

Art. 4*.4 Verifica delle attività*

L´operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un´attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

12. SANZIONI

Disposizioni dell'Autorità Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"

Art.1 Considerazioni preliminari

[Quarto capoverso]

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all´abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques) di recente modifica (V., ad es., l´art. 5 l. 18 marzo 2008, n. 48 che prevede, oltre a una maggiore pena, la procedibilità d´ufficio nel caso in cui il reato sia commesso con "abuso della qualità di operatore del sistema".)

L'inosservanza delle norme comportamentali descritte nel presente documento può comportare l'applicazione di sanzioni disciplinari ovvero di altre misure di tutela dell'Ente che si rendessero necessarie, incluso il risarcimento di eventuali danni arrecati alle apparecchiature, al software ed alle configurazioni in uso.

13. CLAUSOLA DI REVISIONE

Il presente disciplinare abroga e sostituisce integralmente tutti i precedenti adottati in materia.

Il presente disciplinare è aggiornato periodicamente in relazione all'evoluzione tecnologica, organizzativa e della normativa di settore.

14. Appendice A

a. Tabella dei profili di utenze

Descrizione del profilo di utenza	Complessità della password	Scadenza / rinnovo	note
Utente amministratore di base dati generico / default	Lunghezza di almeno 12 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	6 mesi (3 mesi nel caso di servizio esposto sulla rete esterna), da concordare con eventuali fornitori	
Utente amministratore di base dati personale / nominale	Lunghezza di almeno 12 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	3 mesi	
Utente ordinario di base dati	Lunghezza di almeno 8 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	3 mesi	
Utente amministratore di dominio	Lunghezza di almeno 12 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	6 mesi	
Utente amministratore di sistema / server generico / default	Lunghezza di almeno 12 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	6 mesi (3 mesi nel caso di servizio esposto sulla rete esterna), da concordare con eventuali fornitori	
Utente amministratore di sistema personale / nominale	Lunghezza di almeno 12 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	6 mesi	
Utente ordinario di sistema	Lunghezza di almeno 8 simboli; deve	45 giorni	

	comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche		
Utente privilegiato di sistema	Lunghezza di almeno 10 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	45 giorni	Utente con privilegi di amministratore per notebook o pc da utilizzare fuori sede, utente di sistema Linux
Utente VPN	Lunghezza di almeno 12 simboli; deve comprendere maiuscole, minuscole, numeri, simboli di punteggiatura o di operazioni alfanumeriche	6 mesi	
Password di posta elettronica	Lunghezza di almeno 10 simboli, deve comprendere numeri	3 mesi	Pin e PUK generati automaticamente sono sequenze numeriche di 10 simboli
Utente di ownCloud	Lunghezza di almeno 8 simboli; deve comprendere maiuscole, minuscole, numeri	6 mesi	
Credenziali per apparati di rete	Lunghezza di almeno 8 simboli; deve comprendere maiuscole, minuscole, numeri	6 mesi	

15. Appendice B

a. Modello per la richiesta di credenziali, a uso del dirigente responsabile

(da compilare a video e inviare come allegato dalla e-mail del dirigente al Servizio Informatico)

Si richiede l'assegnazione di credenziali per le seguenti risorse a beneficio dell'utente:

Nome	
Cognome	
Ruolo, tipologia contrattuale	
Ditta	
Servizio / Area di ricerca	
Data di attivazione	
Data prevista di cessazione	

☐ Postazione di lavoro

☐ ownCloud

☐ Casella di posta elettronica

☐ VPN

☐ Accesso a Banca Dati

Specificare database: _____

e trattamenti: _____

_____

Data

Il dirigente responsabile