PROVINCIA DI PISA

Istituzione dei Comuni per il governo dell'area vasta Scuole, Strade e Sistemi di trasporto, Territorio e Ambiente Gestione associata di servizi e assistenza ai Comuni

Disciplinare per l'accesso remoto ai sistemi informativi dell'ente

Art.1 Premessa

La Provincia di Pisa gestisce un sistema che consente ai dipendenti di accedere alle risorse informatiche protette, normalmente accessibili solo dalla rete intranet dell'ente, anche da postazioni esterne agli uffici.

L'accesso remoto deve essere preventivamente autorizzato, prevede la disponibilità di credenziali strettamente personali ed è subordinato al rispetto del presente disciplinare, oltre che delle norme civili, penali e amministrative applicabili.

Questo documento è volto a

- definire i criteri di abilitazione al collegamento;
- stabilire le norme comportamentali valide per tutti gli utenti.

Art. 2 Abilitazione all'accesso remoto

Sono abilitati all'accesso remoto:

a) il segretario generale, il capo di gabinetto del presidente, i dirigenti ed i funzionari PO e AP;

b) il personale informatico della UO Tecnologie;

c) i dipendenti autorizzati al lavoro agile con specifico provvedimento del dirigente;

d) i dipendenti autorizzati dal dirigente per motivi di servizio;

Le richieste di cui al precedente punto d) dovranno essere trasmesse alla UO Tecnologie Informatiche, Fonia e Innovazione (di seguito, per semplicità, "UO Tecnologie"), specificando l'eventuale carattere transitorio ed il relativo periodo di validità.

Art. 3 Disposizioni generali

Ogni soggetto che si collega da remoto ai sistemi informativi della Provincia di Pisa assume piena e personale responsabilità delle attività svolte attraverso le credenziali a lui assegnate.

L'utente del sistema di accesso remoto si impegna a:

a) garantire la riservatezza delle proprie credenziali;

b) installare sul proprio telefono personale l'app necessaria per ricevere il codice di autenticazione necessario per il collegamento VPN (vedi seguito);

c) comunicare tempestivamente al Segretario Generale e per conoscenza alla UO Tecnologie lo smarrimento, il furto o l'appropriazione da parte di terzi delle credenziali;

d) segnalare immediatamente alla UO Tecnologie qualsiasi incidente che possa indurre il sospetto di un accesso fraudolento da parte di terzi non autorizzati;

e) accedere esclusivamente ai servizi e ai sistemi informativi per i quali è stato espressamente autorizzato e con le modalità consentite;

f) non recar danno o pregiudizio ai software in dotazione agli uffici dell'ente o a terzi e non interferire con l'utilizzo dei servizi di rete da parte di altri utenti;

g) rispettare la vigente normativa posta a tutela della riservatezza e dei dati personali.

h) rispettare le norme contenute nel presente disciplinare ed utilizzare le credenziali assegnate ai soli fini di fruizione dei servizi a cui è stato autorizzato.

È espressamente vietato utilizzare l'infrastruttura informatica a cui si accede per scopi non strettamente attinenti l'attività lavorativa. In particolare, a titolo esemplificativo e non esaustivo, è vietato:

1) accedere all'infrastruttura informatica dell'ente per conseguire l'accesso a risorse di rete non autorizzate;

2) fornire il servizio di connettività di rete a soggetti terzi non autorizzati all'accesso all'infrastruttura informatica dell'ente;

3) svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni dei sistemi di informatici dell'ente;

4) impedire o interferire o tentare di impedire o interferire in qualsiasi forma con i servizi offerti tramite l'infrastruttura informatica dell'ente ad altri dipendenti;

5) violare la sicurezza di archivi e banche dati; compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.); intercettare, tentare d'intercettare o accedere a dati in transito sull'infrastruttura informatica dell'ente, dei quali non si è destinatari specifici;

6) compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;

7) distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri dipendenti o di terzi; usare, intercettare o diffondere o tentare di usare, intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri dipendenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;

8) creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno.

Art. 4 Misure di sicurezza e modalità di accesso

In base alle direttive nazionali sulla sicurezza informatica emanate dal governo e in linea con le misure minime di sicurezza ICT promosse da AGID, si rende necessario fornire opportuni requisiti di sicurezza al fine di fornire misure tecniche ed organizzative per la protezione dei dati e delle informazioni trattate.

L’accesso remoto alla rete dell’ente è implementato mediante collegamenti protetti su rete privata virtuale (VPN, Virtual Private Network). Per effettuare l’accesso è necessario utilizzare il software Client VPN preventivamente installato e configurato da parte della UO Tecnologie. Sono previsti diversi livelli di autenticazione:

1) tramite password sicura o certificato digitale preconfigurato nel programma;
2) tramite le credenziali personali dell’utente (autenticazione debole);
3) tramite secondo fattore di autenticazione (autenticazione forte) quale one-time password (OTP) veicolata tramite token virtuale o email inviata sulla casella di posta istituzionale (consultabile da rete Internet ad es. tramite la WebMail);

Le specifiche politiche di autenticazione saranno stabilite dal Responsabile per la Transizione al Digitale su proposta del responsabile della UO Tecnologie in base a criteri tecnici, organizzativi e di fattibilità operativa. In generale l’autenticazione forte sarà implementata in tutti i casi in cui ciò risulti fattibile. In caso di autenticazione forte si privilegerà inoltre l’uso del token virtuale rispetto al token via email.

Nel caso autenticazione forte tramite token virtuale l’utente dovrà installare sul proprio telefono una specifica app (disponibile sia per sistema operativo iOS che Android) tramite la quale ricevere il codice OTP.

a) Accesso tramite notebook aziendale

Su tutti i notebook dell’ente assegnati agli utenti come postazioni di lavoro è garantita dall’ente l’attivazione delle misure di sicurezza minime obbligatorie, ed in particolare:

- l’installazione di un sistema operativo aggiornato;
- l’installazione del programma antivirus aggiornato e funzionante;
- l’attivazione di un profilo utente individuale collegato ad un account di dominio e protetto da una password sicura.

Una volta stabilito il collegamento VPN, l’utente potrà fruire di tutti i servizi di rete direttamente dal proprio PC, come se si trovasse in ufficio.

b) Accesso tramite PC personale

In considerazione delle difficoltà e dei costi connessi all’assegnazione di un notebook quale postazione di lavoro, i dipendenti sono autorizzati ad utilizzare per il collegamento ed il lavoro i Personal computer personali a condizione che vengano garantite le seguenti misure di sicurezza minime:

- l’utilizzo di un sistema operativo dotato di licenza d’uso, supportato dal produttore e regolarmente aggiornato con le patch di sicurezza;
- l'installazione sul PC di un software antivirus funzionante e regolarmente aggiornato, con scansioni periodiche schedulate;
- l’abilitazione del firewall personale, se presente;
- l'utilizzo di un account di sistema operativo esclusivamente dedicato all’attività lavorativa e protetto da una password complessa (lunghezza almeno 8 caratteri, combinazione di lettere maiuscole, minuscole, almeno una cifra e almeno un carattere speciale) e modificata almeno ogni 3 mesi; si raccomanda che la password non contenga riferimenti a nomi di persone riconducibili all’utente o ad ambiti noti;

L’utente autorizza i tecnici della UO Tecnologie e di eventuali terze parti incaricate dall’ente ad effettuare periodicamente le verifiche di idoneità sui suddetti requisiti.

Fatto salvo il software Client VPN, sul PC personale utilizzato non dovrà essere installato alcun software dell’ente in quanto esso svolge solo la funzione di terminale remoto verso il desktop presente in ufficio.

Dovranno essere rispettate le seguenti disposizioni:

1) collegarsi alla rete Internet tramite la propria connessione domestica fissa o mobile, non utilizzare connessioni Wi-Fi pubbliche;
2) avviare il Client VPN per stabilire la connessione sicura con la rete dell’ente ed immettere le chiavi di accesso, così come richiesto dal programma;
3) avviare il programma Desktop Remoto per il collegamento al desktop aziendale previa ulteriore autenticazione con le proprie credenziali di dominio;
4) operare dal proprio desktop aziendale sui programmi, i dati ed i documenti nel rispetto di tutte le misure di sicurezza in vigore all'interno dell'ente, come se si trovasse sul posto di lavoro (la riservatezza è garantita in quanto il desktop in ufficio risulta bloccato e non è possibile visualizzare le attività svolte);
5) non cliccare su link o allegati contenuti in e-mail sospette;
6) non utilizzare dispositivi mobili (pen drive e hard disk esterni) di cui non si conosce la provenienza;
7) salvare e/o condividere dati in archivi personali o su risorse cloud non autorizzate espressamente dall’ente;
8) bloccare la propria postazione informatica in tutte le occasioni in cui ci sia necessità di allontanamento anche temporaneo dalla stessa;
9) chiudere il collegamento VPN ad ogni pausa di lavoro e riaprirlo alla successiva ripresa;
10) al termine dell’attività lavorativa spegnere da remoto il PC dell’ufficio e chiudere il collegamento VPN.

È espressamente vietato installare software contraffatto o proveniente da fonti non ufficiali.

Art. 5 Utilizzo del notebook aziendale

Il dipendente che dispone di un notebook aziendale assegnato quale postazione di lavoro potrà essere autorizzato dal proprio dirigente al trasporto e all'impiego fuori dalla sede di lavoro ferme restando le seguenti condizioni:

1. I beni assegnati rappresentano un mezzo di lavoro e devono essere utilizzati esclusivamente per lo svolgimento delle mansioni lavorative, come regolate dalle disposizioni organizzative dell’ente, in base a principi di massima correttezza e professionalità, nel rispetto della normativa vigente; ciò perché ogni uso anomalo può comportare rischi per l’ente e per il lavoratore.
2. Data la loro tipologia e fermo restando quanto sopra indicato, le attrezzature possono essere trasportate ed utilizzate anche fuori dalla sede di lavoro. Il consegnatario si obbliga a conservare e a custodire i beni in oggetto con cura e massima diligenza, a non destinarli ad altri usi che non siano quelli sopra previsti, ed a restituirli nello stato attuale, salvo il normale deterioramento d’uso.
3. L’assegnazione delle attrezzature dà luogo alle forme di responsabilità previste dalla legge e dai regolamenti per i consegnatari dei beni mobili come individuati nell’articolo 812 del

Codice Civile. Il consegnatario del bene mobile, è agente responsabile della tutela dei beni a lui affidati ed è quindi responsabile della custodia, della diligente conservazione e dell'uso appropriato, dal momento della di presa in carico al momento della restituzione.

4. Il consegnatario è l'unico responsabile di fronte all'autorità pubblica in caso di smarrimento o furto. I casi di danno intenzionale, danno colposo, smarrimento o furto dei beni saranno disciplinati in base all'ordinamento dell'ente.
5. Ogni bene assegnato è, e resterà, di esclusiva proprietà dell'Ente; la lettura ed approvazione del presente documento, dunque, rappresenta la rinuncia a qualsiasi tipo di rivalsa sul bene stesso. Il dirigente della struttura di appartenenza può revocare l'assegnazione in qualunque momento, sia in caso di utilizzo non corretto che per motivi di servizio, senza obbligo di motivazione.
6. L'utilizzatore è personalmente responsabile del computer, è fatto assoluto divieto di cessione a terzi o di consentirne l'utilizzo da parte di terzi. In caso di allontanamento durante una sessione di lavoro l'utilizzatore deve attivarsi per renderla inaccessibile a terzi. L'utilizzatore deve inoltre provvedere all'archiviazione periodica dei dati, che sono di proprietà dell'ente, anche tramite salvataggio sulle condivisioni di rete messe a disposizione dall'ente.
7. E' fatto divieto di installare e/o utilizzare programmi diversi da quelli forniti o autorizzati dal datore di lavoro, il quale provvede alle licenze d'uso. E' vietato modificare la configurazione del computer, disinstallare o disattivare i programmi, senza previa autorizzazione. Il personale tecnico incaricato ed autorizzato dall'ente potrà effettuare verifiche automatizzate o puntuali sui software e sulle componenti hardware e software del computer per scopi di manutenzione e assistenza.

Durante l'utilizzo nella sede di lavoro si raccomanda:

- in caso di allontanamento dalla propria postazione, agganciare il notebook al lucchetto (kensington lock) eventualmente fornito in dotazione (da assicurare stabilmente alla scrivania) e bloccare lo schermo;

- al termine dell'utilizzo chiudere a chiave il notebook in una cassettiera o un armadio, oppure lasciarlo ancorato al lucchetto e opportunamente celato; se possibile chiudere a chiave l'ufficio.

Art. 6 Monitoraggio

Il Segretario Generale, avvalendosi della UO Tecnologie, effettuerà il monitoraggio e la misura delle attività di rete originate dalle credenziali assegnate, al fine di garantirne funzionalità e affidabilità, nel rispetto del principio di pertinenza e non eccedenza, secondo quanto previsto dalla normativa vigente (D. Lgs. 196/2006 e SS.MM.II. e Regolamento UE 2016/679).

Art. 7 Violazioni

La Provincia di Pisa, nella persona del Segretario Generale e avvalendosi della UO Tecnologie, adotta ogni misura necessaria per prevenire, reprimere e punire violazioni al presente disciplinare. Chiunque abbia notizia di una violazione, avvenuta o temuta, è tenuto a segnalarlo immediatamente al Segretario Generale per i provvedimenti del caso. Il Segretario Generale può ordinare l'immediata cessazione dell'attività all'origine dell'abuso, adottando le necessarie misure per impedire ulteriori conseguenze ed individuare il responsabile. In particolare, si riserva di sospendere e/o revocare le credenziali assegnate nel caso in cui venga rilevato un uso non corretto e comunque non conforme al presente Regolamento, notificando al dipendente ed al Dirigente responsabile le motivazioni di tale decisione. Accertata l'esistenza della violazione, il Segretario Generale - sentito

il dipendente cui è imputata la violazione stessa - lo esclude temporaneamente o permanentemente, dall'accesso VPN. Sono fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa e disciplinare della violazione compiuta. In particolare, si rammenta che i comportamenti illeciti che integrano gli estremi di reati informatici ed elettronici, ai sensi della legge 48/2008 sono perseguibili dall'autorità giudiziaria e puniti a norma della legge penale.

Art. 8 Disposizioni finali ed entrata in vigore

Per tutto quanto non espressamente contemplato dal presente disciplinare, valgono le disposizioni previste dalla normativa vigente in materia e dal Regolamento Uffici e Servizi.

Il presente disciplinare entrerà in vigore ad avvenuta esecutività del relativo atto di approvazione.