

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI DELL'ORDINE ARCHITETTI P.P.C. PROVINCIA DI VICENZA– DI SEGUITO DETTO ANCHE ENTE

Approvato dal Consiglio nella seduta del 22.02.2021 (DELIBERA N. 9)

Indice

Premessa

1. Entrata in vigore del regolamento e pubblicità
2. Campo di applicazione del regolamento
3. Utilizzo del Personal Computer
4. Gestione ed assegnazione delle credenziali di autenticazione
5. Utilizzo della rete
6. Utilizzo e conservazione dei supporti rimovibili
7. Utilizzo di PC portatili
8. Uso della posta elettronica
9. Navigazione in Internet
10. Protezione antivirus
11. Utilizzo dei telefoni, fax e fotocopiatrici dell'Ente
12. Osservanza delle disposizioni in materia di Privacy
13. Accesso ai dati trattati dall'utente
14. Sistema di controlli graduali
15. Sanzioni
16. Aggiornamento e revisione

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'ente e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Ente ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Tali prescrizioni si manifestano come mezzo idoneo a concretare il dovere di accountability di cui al GDPR (Reg. Eu. N. 2016/679) a carico del Titolare del Trattamento dati, ciò sino ad un ulteriore adeguamento da parte del Garante della Privacy.

1. Entrata in vigore del regolamento e pubblicità

- 1.1 Il nuovo regolamento entrerà in vigore il 01.04.2021. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate se non conformi e sostituite dalle presenti.
- 1.2 Copia del regolamento verrà consegnato a ciascun dipendente.

2. Campo di applicazione del regolamento

- 2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'ente ed al personale somministrato e/o appaltato a prescindere dal rapporto contrattuale con la stessa intrattenuto (volontari, lavoratori somministrati, collaboratore a progetto, in stage, ecc.).
- 2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

3. Utilizzo del Personal Computer

- 3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro.** Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
- 3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'ente solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.
- 3.3 L'Ente rende noto che il personale incaricato che opera presso il servizio Information and Communication Technology (nel seguito per brevità "Servizio ICT") dello stesso è stato autorizzato a compiere interventi nel sistema informatico dell'Ente diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

- 3.4 Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
- 3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio ICT per conto dell'ente né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'ente stesso a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
- 3.6 Salvo preventiva espressa autorizzazione del personale del Servizio ICT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).
- 3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio ICT nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.
- 3.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In caso di necessità di operare da remoto (smart working) il computer presente presso la sede dell'Ordine dovrà essere lasciato acceso ma in stato di standby con screen saver attivo.
- 3.9 Il personale non deve mai digitare comandi su un computer su richiesta di terzi non verificati.
- 3.10 Il personale non deve mai rivelare informazioni sulle caratteristiche dei sistemi informatici su richiesta di terzi non verificati.
- 3.11 Il personale non deve mai aprire/scaricare applicazioni e/o programmi su richiesta di terzi non verificati.

4. Gestione ed assegnazione delle credenziali di autenticazione

- 4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Consiglio Direttivo o dal Responsabile dell'ufficio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.
- 4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà venir

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio ICT.

- 4.3 La parola chiave, deve essere formata da lettere (maiuscole e minuscole), da numeri e caratteri speciali (come %, !, £ ecc.) in combinazione fra loro, e deve essere composta da almeno otto caratteri. Non deve contenere riferimenti agevolmente riconducibili all'incaricato, parole del vocabolario in qualsiasi lingua e non deve essere una variante di una parola chiave già usata.
- 4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi.
- 4.5 La password non può essere cambiata su richiesta di persona diversa dal Consiglio Direttivo o dal punto di contatto del servizio IT.
- 4.6 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.
- 4.7 In nessun caso chi usa un computer rivelerà le credenziali di autenticazione per un qualsiasi motivo senza previo consenso scritto del Consiglio Direttivo.
- 4.8 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del Servizio ICT dell'Ente. Il personale deve appuntare le password soltanto quando le conserva in un posto sicuro lontano dal computer. In ogni caso, le password in chiaro non saranno registrate in alcun file.
- 4.9 Il personale non deve mai usare in un sito web una password identica o simile a quella che usa sul computer dell'Ente. Ciò vale anche per la navigazione on-line svolta nella propria vita privata.
- 4.10 Il personale non deve mai usare una password identica o simile in più di un sistema (computer, e-mail, router, firewall, applicazioni varie). Ciò vale anche per la navigazione on-line svolta nella propria vita privata.

5. Utilizzo della rete dell'Ente

- 5.1 Per l'accesso alla rete dell'Ente ciascun utente deve essere in possesso della specifica credenziale di autenticazione.
- 5.2 Le credenziali di autenticazione per l'accesso alla rete dell'Ente non devono mai essere comunicate all'esterno.
- 5.3 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. La parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- 5.4 Le cartelle utenti presenti nei server dell'Ente sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio ICT.

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

- 5.5 Il personale del Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
- 5.6 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

- 6.1 Tutti i supporti magnetici rimovibili (supporti USB, ecc.) esclusivamente dell'Ente, contenenti dati particolari ai sensi del GDPR nonché informazioni costituenti know-how dell'ente, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- 6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.
- 6.3 In ogni caso, i supporti magnetici contenenti dati particolari ai sensi del GDPR devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
- 6.4 E' vietato l'utilizzo di supporti rimovibili personali.
- 6.5 L'utente è responsabile della custodia dei supporti e dei dati dell'Ente in essi contenuti.

7. Utilizzo di PC portatili

- 7.1 L'utente è responsabile del PC portatile assegnatogli dal Servizio ICT e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
- 7.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
- 7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8. Uso della posta elettronica

- 8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- 8.2 È fatto divieto di utilizzare le caselle di posta elettronica assegnata dall'ente per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
 - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

- 8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- 8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'ente ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogo dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.
- 8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.
- 8.6 È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). In ogni caso essi non devono essere aperti se non sono attesi per necessità lavorative o se non provengono da persona fidata.
- 8.7 Al fine di garantire la funzionalità del servizio di posta elettronica dell'Ente e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente.
- 8.8 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura dell'azienda.
- 8.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 8.8).
- 8.10 Il personale del servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.
- 8.11 Al fine di ribadire agli interlocutori la natura esclusivamente dell'Ente della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dell'ente potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy dell'Ente.

9. Navigazione in Internet

- 9.1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell'Ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

- 9.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio ICT);
 - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o del Servizio ICT) e comunque nel rispetto delle normali procedure di acquisto;
 - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
 - la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
 - l'accesso, tramite internet, a caselle webmail di posta elettronica personale.
- 9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'ente rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.
- 9.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 3 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.
- 9.5 Il personale non può divulgare attraverso i social media informazioni riservate, come la corrispondenza interna, informazioni di terze parti di cui è a conoscenza (ad esempio partner, istituzioni, utenti, stakeholder ecc.) o informazioni su attività lavorative, servizi, progetti e documenti.
- 9.6 Il personale deve astenersi dal trasmettere e diffondere messaggi minatori o ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti dell'azienda.
- 9.7 Il personale non può divulgare foto, video, o altro materiale multimediale, che riprenda locali e personale senza l'esplicita autorizzazione delle strutture e delle persone coinvolte (ad eccezione di eventi pubblici che si svolgono nella sede di lavoro).

10. Protezione antivirus

- 10.1 Il sistema informatico dell'ente è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Ente mediante virus o mediante ogni altro software aggressivo.
- 10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

- 10.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

11. Utilizzo dei telefoni, fax e fotocopiatrici dell'Ente

- 11.1 Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso dell'Ente a disposizione.
- 11.2 Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare dell'Ente si applicano le medesime regole sopra previste per l'utilizzo del telefono dell'Ente: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS o messaggi diversi di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'uso promiscuo non è autorizzato.
- 11.3 È vietato l'utilizzo dei fax dell'Ente per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.
- 11.4 È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

12. Miscellanea

- 12.1 I numeri di telefono e gli indirizzi e-mail dei singoli collaboratori IT non saranno rivelati a terzi non espressamente autorizzati.
- 12.2 Nessun dipendente disabiliterà alcun apparecchio di rete o porte seriali per conto di tecnici non verificati.
- 12.3 I nomi dei dipendenti che hanno segnalato problemi legati al computer non devono essere diffusi all'esterno.
- 12.4 I dipendenti che sospettano di essere stati oggetto di una violazione di sicurezza, comprese richieste di rivelare informazioni o eseguire azioni su un computer, devono riferire immediatamente il fatto al diretto superiore o al Consiglio Direttivo.
- 12.5 I dipendenti non parteciperanno ad indagini telefoniche.

13. Osservanza delle disposizioni in materia di Privacy

- 13.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D.Lgs. n. 196/2003 e del Regolamento Ue n. 2016/679 (c.d. GDPR).

14. Accesso ai dati trattati dall'utente

ORDINE DEGLI ARCHITETTI, PIANIFICATORI, PAESAGGISTI E CONSERVATORI DELLA PROVINCIA DI VICENZA

14.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi dell'Ente (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Consiglio Direttivo, tramite il personale del Servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici dell'Ente e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

15. Sistemi di controlli gradualità

15.1 In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti dell'Ente e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

15.2 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL e dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dall'ente.

17.2 Il presente Regolamento è soggetto a revisione con frequenza biennale.

Vicenza, lì 22 Febbraio 2020

ORDINE ARCHITETTI P.P.C. PROVINCIA DI VICENZA

