Allegato "A"

DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELLA PROVINCIA DI MODENA

Parte I – Aspetti generali e comportamentali 2

Art. 1 Finalità del presente documento 2
Art. 2 Ambito di applicabilità 2
Art. 3 Definizioni 2
Art. 4 Sicurezza fisica dei locali 3
Art. 5 Accesso e utilizzo delle postazioni di lavoro 3
Art. 6 Accesso dall'esterno 3
Art. 7 Utilizzo delle postazioni di lavoro 4
Art. 8 Utilizzo di dispositivi mobili 4
Art. 9 Utilizzo del software 5
Art. 10 Assegnazione delle caselle di posta elettronica 5
Art. 11 Utilizzo e gestione della posta elettronica 5
Art. 12 Navigazione internet 6
Art. 13 Utilizzo di applicazioni internet su dispositivi fissi e mobili 6
Art. 14 Attività di supporto del servizio informatico 7
Art. 15 Attività di supporto di software house e fornitori esterni 7
Art. 16 Accesso ai dati e alle risorse di rete 7
Art. 17 Gestione dei registri degli accessi 8
Art. 18 Tutela della Privacy 8

Parte II – Aspetti organizzativi ed economici 8

Art. 19 Architettura complessiva dei sistemi informativi. 8
Art. 20 Acquisizione di nuovi sistemi informativi 9
Art. 21 Comitato Servizio Informatico …….. 9

Parte III - Disposizioni finali e trasitorie 9

Art. 22 Modalità di diffusione del presente documento 9

Parte I – Aspetti generali e comportamentali

Art. 1 Finalità del presente documento

Il presente documento rientra tra le misure minime adottate dalle amministrazioni in attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri e intende fornire indicazioni tecniche ed organizzative da applicare per garantire la sicurezza dei dati trattati con strumentazioni informatiche.
Finalità del presente documento è permettere una crescita tecnologica ed organizzativa dei sistemi informativi del Provincia di Modena, in un'ottica di sviluppo, al fine di estendere l'uso delle tecnologie sia nell'organizzazione dell' ente che nel rapporto con cittadini, professionisti e imprese, senza mettere a rischio la sicurezza dell'intero sistema; la corretta applicazione di regole comuni e condivise ha lo scopo di impedire, o comunque ridurre il rischio che eventuali problemi di sicurezza su una postazione o su un punto della rete si propaghino sfruttando l'interconnettività e l'interdipendenza fra le componenti del sistema informativo dell'Ente.

Art. 2 Ambito di applicabilità

L'ambito di applicabilità è esteso a tutti i soggetti che utilizzano postazioni di lavoro e operano sui dati e sulle informazioni contenute in elaboratori elettronici, che hanno accesso ad archivi e a documenti cartacei, alla rete dell'Ente e ai sistemi informatici della Provincia di Modena: dipendenti, collaboratori, amministratori, imprese che hanno rapporti contrattuali con l'Ente o altri soggetti che ne abbiano titolo.
Quanto riportato nel presente documento non esaurisce la disciplina applicabile, dovendosi garantire il rispetto di tutte le prescrizioni contenute nelle vigenti normative civili e penali.

Art. 3 Definizioni

Di seguito vengono fornite alcune definizioni per rendere più comprensibile il documento.
Sistema Informativo: complesso di strumentazioni hardware e sistemi software. **Struttura Sistemi Informativi (di seguito SI):** organizzazione all'interno dell'Ente che gestisce la funzione informatica del Provincia di Modena che corrisponde alla parte informatica del Servizio Personale e sistemi informativi e telematica
Rete interna: rete informatica accessibile dai locali del Provincia di Modena.
Rete esterna: rete pubblica a cui accedono ordinariamente cittadini, imprese e professionisti, in sostanza la rete Internet.
Firewall: dispositivi fisici o logici che separano la rete esterna da quella interna ai fini di proteggere la rete interna.
Utilizzatori dei sistemi informativi: dipendenti, collaboratori stabili (stagisti, borse lavoro, contratti di lavoro temporaneo), amministratori (Presidente e Consiglieri).
Gli utilizzatori accedono con profili diversi al sistema in base alle funzioni svolte sia di tipo tecnico che politico.
Utilizzatori occasionali: sono soggetti che accedono occasionalmente alla rete interna, quali ad esempio fornitori.
Operatori del servizio informatico: tecnici del servizio informatico che con profili diversi svolgono le funzioni di amministratore dei sistemi informatici: rete, server, database, ecc.
Postazione di lavoro (o postazione client): computer fisso o mobile utilizzato per l'attività lavorativa.
Postazione di lavoro virtuale: computer a cui non è associabile in modo diretto un sistema hardware accessibile fisicamente all'utilizzatore; la postazione di lavoro virtuale

viene utilizzata solitamente con un collegamento di una postazione fisica e ha le stesse funzionalità della postazione di lavoro ordinaria.
Server: computer utilizzato per fornire servizi a più utilizzatori della rete interna. Non prevede di solito la connessione diretta degli utilizzatori come avviene per le postazioni di lavoro fisiche o virtuali.
Data Center: struttura utilizzata per alloggiare sistemi informatici costituiti da server, dispositivi di archiviazione e apparati di telecomunicazioni.
Sistema di LOG : insieme di file che raccolgono gli eventi di un determinato programma o sistema, esempio il flusso di posta elettronica inviata e ricevuta o siti internet visitati, in caso di indagini per reati informatici http://www.commissariatodips.it la polizia postale ne richiede la visione.
GDPR: Regolamento (UE) 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 (di seguito GDPR) il quale ha abrogato la direttiva 95/46/CE
Coordinatore interno per la protezione dei dati: ai sensi del nuovo GDPR, è persona fisica interna all'Ente, nominata dal Titolare al trattamento di dati personali (art. 29 D. Lgs. n. 196/2003).
Responsabile del trattamento: ai sensi del nuovo GDPR è la persona fisica o giuridica che effettua i trattamenti per conto del titolare designata con apposito atto dal Titolare stesso o da suo delegato ai sensi dell'art. 28 del GDPR stesso.

Art. 4 Sicurezza fisica dei locali

L'accesso ai locali e alle postazioni di lavoro è riservato agli utilizzatori in base alle funzioni loro assegnate. L'apertura e la chiusura delle sedi e l'accesso agli uffici durante gli orari di apertura al pubblico è affidata agli addetti alla portineria o a personale preposto.
Al di fuori degli orari di apertura, l'accesso è consentito al personale autorizzato.
Di sera la sorveglianza viene effettuata attraverso un sistema d'allarme collegato con la Ditta affidataria del sistema di vigilanza.
L'accesso di personale esterno (quale, ad esempio, fornitori dell'Ente), che per necessità dovesse utilizzare in modo estemporaneo la postazione di lavoro, dovrà essere concordato e autorizzato dalla Struttura Sistemi Informativi ed avviene sotto la responsabilità dell'utilizzatore interno che ne richiede l'intervento.

Art. 5 Accesso e utilizzo delle postazioni di lavoro

L'accesso alle postazioni di lavoro avviene con account (credenziale) personale e nominativa, ad esclusione di quelle postazioni che, per particolari esigenze di rotazione, consentono l'accesso con un account che identifica il servizio.
La parte riservata delle credenziali di accesso (password, pin o altro) viene modificata periodicamente dall'operatore su segnalazione del sistema in base alle disposizioni della normativa vigente. Ogni utilizzatore è responsabile della custodia delle password e delle altre credenziali personali di accesso ai sistemi. E' fatto divieto di comunicare, o rendere facilmente accessibili, i propri identificativi personali a soggetti terzi.
Se l'operatore dimentica la password è fatto obbligo di comunicarlo all'amministratore di Sistema che provvede in merito.
Le postazioni di lavoro sono fornite dall'Ente. Gli utilizzatori non possono attivare postazioni di lavoro di proprietà nella rete interna, salvo specifica autorizzazione del SI.
L'abilitazione alla rete interna permette l'utilizzo di tutte le postazioni di lavoro fisiche o

virtuali. Le autorizzazioni sono assegnate agli utenti e non alle postazioni che sono tendenzialmente intercambiabili, almeno per le funzioni di base.
Quando un utente cessa il servizio presso l'ente, deve essere tempestiva comunicazione al SI da parte del servizio Personale e il suo accesso non può essere ceduto ad un altro utente; i dati di interesse del servizio in accordo tra l'utente e il SI devono essere memorizzati sulle cartelle di rete condivise. L'accesso verrà disattivato dal SI alla ricezione della comunicazione e verrà cancellato definitivamente dopo 30 giorni.

Art. 6 Accesso dall'esterno

L'accesso alla rete interna dall'esterno in generale è vietato; può essere abilitato solo a seguito di specifica richiesta scritta:

– per gli amministratori e i responsabili apicali da parte dell'interessato;
– per i dipendenti che non abbiano funzioni apicali da parte del responsabile apicale dell'area di riferimento.

L'accesso non è immediato ed automatico, ma avviene dopo l'esito favorevole di un'istruttoria effettuata dall'SI allo scopo di verificare le prestazioni minime indispensabili della connettività utilizzata; oltre a ciò, l'accesso è autorizzato solo tramite postazioni di lavoro fornite dall'ente.

Art. 7 Utilizzo delle postazioni di lavoro

La proprietà delle postazioni di lavoro è dell'Amministrazione Provinciale di Modena e l'utilizzo è consentito unicamente per i fini lavorativi e istituzionali inerenti l'utilizzatore.
L'utilizzo della postazione di lavoro e, in genere, degli strumenti informatici, non configura alcuna titolarità da parte dell'utilizzatore degli strumenti stessi né dei dati e delle informazioni trattate. E' vietato caricare e detenere nelle postazioni di lavoro, materiale non attinente con l'attività lavorativa o istituzionale.
Gli utilizzatori salvano i dati nelle unità di rete appositamente predisposte; non è garantito il salvataggio dei dati memorizzati sulla postazione di lavoro locale, né è garantito il passaggio di tali dati, in caso di sostituzione della postazione. I dati memorizzati sulla postazione di lavoro locale non sono soggetti a nessuna politica di backup. Ogni utilizzatore è responsabile del salvataggio dei dati memorizzati.
Gli operatori possono richiedere anche l'attivazione di una cartella personale, sempre sul server di rete, nella quale poter memorizzare dati che richiedono il massimo livello di riservatezza. La quota per ciascuna cartella è di 50 Gb.
Per particolari esigenze di servizio, dovranno essere adottate specifiche politiche di salvataggio dei dati per gli operatori che utilizzano le postazioni di lavoro mobili in accordo con il servizio informatico.
Alla fine della sessione di lavoro gli utilizzatori spengono la postazione oppure, in subordine, effettuano la semplice disconnessione dalla rete, lasciando acceso il computer, nel caso siano necessari collegamenti remoti successivi.
In caso di momentaneo abbandono della postazione di lavoro, qualora ciò non avvenga automaticamente, gli utilizzatori sono tenuti a bloccare la postazione stessa in modo che l'accesso non sia consentito a soggetti non autorizzati.
L'utilizzatore deve custodire ed utilizzare la postazione di lavoro e, in genere, gli strumenti informatici affidatigli con la massima attenzione e diligenza, anche al fine di tutelare la sicurezza del sistema.
La postazione di lavoro non può essere collocata al pavimento o in posizioni che ne possono compromettere il funzionamento, (adiacenti a stufe elettriche o termosifoni, a piante che vengono regolarmente annaffiate, sotto finestre aperte).

La postazione di lavoro non deve mai essere scollegata dalla rete e sostituita da altri dispositivi da personale non autorizzato da SI, e neppure collegate a reti diverse da quella per la quale la postazione è identificata.

Art. 8 Utilizzo di dispositivi mobili

Anche nell'utilizzo di dispositivi mobili devono essere assicurate la cura e la diligenza di cui al precedente art.7.

L'utilizzo delle postazioni di lavoro portatili e mobili (notebook, tablet, smartphone) richiede inoltre maggiori precauzioni rispetto alle postazioni fisse in ordine ai seguenti elementi: attenzione rispetto al furto o allo smarrimento delle stesse;
attenzione rispetto a virus o codici maligni tramite reti wireless (senza fili).
Le postazioni di lavoro mobili vengono acquistate per esigenze di lavoro specifiche in cui l'utilizzatore ha necessità di frequenti spostamenti o per l'utilizzo in smartworking, ed assegnate in accordo con i responsabili dei servizi interessati. Si ribadisce il divieto di installare sulle postazioni mobili software non compresi nell'elenco di cui all'art.9.

Art. 9 Utilizzo del software

Ogni necessità di software sulla postazione di lavoro deve essere comunicata a SI, la quale provvederà a redigere, pubblicare ed aggiornare l'elenco dei software autorizzati, oltre ovviamente ad installare il software sulle postazioni richieste.
L'utilizzo del software avviene nel rispetto del diritto d'autore. Chi richiede l'installazione di un software deve avere acquisito la licenza d'uso ove prevista, o comunque fornire agli operatori SI i relativi termini di licenza o d'uso.
Vige il divieto assoluto di installazione di software da parte degli utilizzatori, salvi differenti e specifici accordi con SI; tale attività è riservata agli operatori SI che ne verificano preventivamente la compatibilità con i sistemi esistenti.

Art. 10 Assegnazione delle caselle di posta elettronica

I dipendenti e i collaboratori che utilizzano le postazioni di lavoro della rete interna hanno a disposizione una propria casella di posta elettronica o d'ufficio in base ai criteri organizzativi definiti dall'Ente.
Per attivare la condivisione di una casella di posta (solitamente d'ufficio) che deve essere consultata da più persone, il responsabile del servizio inoltra apposita richiesta al SI, che attiva il meccanismo di condivisione via software; il responsabile del servizio ha anche il compito di comunicare eventuali variazioni riguardanti le condivisioni ed eventuali utenti non più attivi nel suo servizio. Alla casella di posta condivisa ogni utilizzatore accede con le proprie credenziali
A tutti i dipendenti, viene fornita una casella di posta elettronica personale e individuale, fatti salvi specifici impedimenti di natura tecnica e organizzativa del soggetto interessato.
I dipendenti sono tenuti ad utilizzare la casella di posta assegnata per le comunicazioni con l'Ente preferendola rispetto ad altre caselle fornite da soggetti esterni (ad esempio per le comunicazione con l'ufficio personale).

Art. 11 Utilizzo e gestione della posta elettronica

La casella di posta elettronica assegnata, personale o relativa all'ufficio, contiene nella parte relativa al dominio il riferimento all'ente di appartenenza e costituisce uno strumento di lavoro. L'utilizzo della casella assegnata avviene per fini istituzionali o per comunicazioni personali attinenti l'attività lavorativa.

Ai fini del corretto utilizzo della posta elettronica, gli utenti delle caselle di posta devono rispettare alcune semplici regole:

- nell'invio della posta elettronica gli utenti devono includere tra i destinatari solo gli indirizzi strettamente necessari e cercare di limitare la diffusione di indirizzi di posta elettronica di colleghi o terzi, in quanto tale operazione favorisce la diffusione dello spamming (mail spazzatura);
- per lo stesso motivo e per l'inutile occupazione di spazio sui server sono vietate le cosiddette "Catene di Sant'Antonio" ovvero l'inoltro a varie persone di messaggi che contengono informazioni anche se riferite a iniziative lodevoli
- è fatto divieto di utilizzare la casella di posta rilasciata dall'ente per iscriversi a servizi di vendita e/o offerte, newsletter e similari non attinenti al proprio servizio;
- è buona norma attivare per lo stretto tempo necessario, la funzione fuori ufficio, qualora ci si assenti dal servizio;
- quando un utente cessa il servizio presso l'ente, deve essere inviata dal Servizio Personale comunicazione al SI e la sua casella di posta personale non può venire ceduta ad un altro utente; deve essere invece attivato il messaggio di *"fuori ufficio"* a cura dell'utente stesso che indichi chiaramente che il dipendente non è più in servizio;

Il SI definisce le politiche per la conservazione e l'archiviazione dei messaggi di posta elettronica in modo da permetterne la corretta fruizione da parte degli utilizzatori nel rispetto dell'equilibrio complessivo e dimensionamento dei sistemi.
La posta elettronica è un sistema di comunicazione e non di archiviazione delle informazioni, pertanto gli utilizzatori devono, al fine di un migliore utilizzo globale, limitare la crescita della dimensione complessiva della casella, effettuando periodicamente la cancellazione delle email non più necessarie.
Il SI attiva funzioni di controllo antispam e antivirus sui messaggi di posta elettronica sia in entrata che in uscita e traccia attraverso sistema di LOG tutte le mail che transitano sul sistema di posta.

Art. 12 Navigazione internet

Come prescritto dal Piano Triennale per l'informatica nella Pubblica Amministrazione (cap.3.2) è garantito "l'accesso alla rete Internet a **tutti i dipendenti della PA**, indipendentemente dal ruolo o dai compiti assegnati e senza limiti di tempo o orari.
Internet oggi deve essere considerato a tutti gli effetti uno strumento di lavoro indispensabile ed efficace per svolgere ogni tipo di attività: dal trovare numeri di telefono, all'identificare persone e relazioni tra queste persone, riferimenti di un concorso o normativi, documentazione tecnica, strumenti di produttività (traduzioni, orari nel mondo, ecc.), servizi di emergenza o notizie di ogni tipo."
L'accesso a social network, forum, chat o simili è consentito unicamente, previa analisi appunto delle necessità organizzative, su richiesta del responsabile del servizio e in accordo con il SI su tempi e modi di attivazione. E' comunque vietato utilizzare i profili social personali per agire in nome e per conto dell'Ente o utilizzare i profili social dell'Ente per fini personali, politici o commerciali.
La navigazione in internet è uno strumento di lavoro ed è consentita per finalità attinenti o comuque connesse all'attività lavorativa, fatti salvi i casi di necessità. E' comunque vietato l'uso reiterato o prolungato per fini personal. Il SI predispone un servizio di filtro automatico dei contenuti (content filtering) finalizzato ad evitare siti potenzialmente dannosi e dal contenuto pericoloso. Il sistema di content filtering è aggiornato automaticamente sulla base di un software che tiene conto delle principali black list pubblicate sul web; tale sistema non esaurisce l'elenco dei siti sconsigliati, in quanto variabile ad altissima velocità, intende solo fornire una indicazione di massima; ogni

utilizzatore è responsabile sotto il profilo amministrativo, civile, penale e disciplinare del corretto uso della navigazione in internet. Si raccomanda, in particolare, estrema prudenza nel collegamento a siti sconosciuti.
La classificazione automatica dei siti rischiosi può comportare anche il blocco di siti che in realtà non lo sono, pertanto, in caso il blocco riguardi un sito non pericoloso, indispensabile per lo svolgimento delle proprie attività, l'utente può chiedere al SI lo sblocco del sito stesso.
Il SI, conformemente alle normative vigenti, mantiene il log dell'attività di navigazione su tutta la rete; **la consultazione dello stesso log è ammessa solo** dietro richiesta delle autorità di polizia postale secondo le norme vigenti.

Art. 13 Utilizzo di applicazioni internet su dispositivi fissi e mobili
È in generale impedito attraverso content filtering l'utilizzo di programmi ludici, di intrattenimento tramite Internet, file sharing e peer to peer (giochi, chat, ecc.) in quanto tali sistemi, a prescindere dall'impatto sull'attività lavorativa, possono contenere vulnerabilità tali da permettere attacchi informatici con l'obbiettivo di diminuire la sicurezza complessiva del sistema informativo dell'ente.
Chi avesse necessità di utilizzare tali sistemi per fini istituzionali dovrà concordarne preventivamente l'utilizzo con il SI.

Art. 14 Attività di supporto del servizio informatico
Il SI effettua, tramite personale proprio o fornitori di fiducia, l'attività di supporto nell'utilizzo dei sistemi informativi.
Per effettuare assistenza gli operatori del SI utilizzano, nei limiti del possibile, sistemi di accesso e controllo remoto delle postazioni di lavoro. L'accesso remoto alle postazioni di lavoro avviene sempre d'accordo tra l'utilizzatore della postazione e l'operatore del SI.

Art. 15 Attività di supporto di software house e fornitori esterni
I fornitori di software possono fornire assistenza anche tramite collegamenti da remoto secondo le modalità concordate con il SI. Il collegamento avviene in modo presidiato a seguito di specifica autorizzazione degli operatori del SI.
Nel caso in cui l'accesso avvenga da parte di personale incaricato dalle software house senza il tramite degli operatori del SI, deve sempre essere possibile identificare l'operatore che ha effettuato l'accesso.
Qualora i fornitori o altri soggetti esterni debbano effettuare attività sulle postazioni di lavoro degli utilizzatori o sui server per installazioni e configurazioni, tali attività dovranno essere concordate preventivamente con il SI.
La società che fornisce assistenza viene nominata responsabile del trattamento ai sensi dell'art. 28 del GDPR.

Art. 16 Accesso ai dati e alle risorse di rete
L'attivazione di nuovi utenti e le impostazioni per l'accesso ai dati vengono effettuate dal personale del SI a seguito di richiesta da parte del Responsabile del servizio di riferimento che provvede, a norma di legge ad aggiornare di conseguenza il registro dei trattamenti, tenuto ai sensi del GDPR.

L’abilitazione alle applicazioni e l’assegnazione di funzioni all’interno dell’applicazione vengono effettuate dal Responsabile relativo al servizio a cui l’applicazione si riferisce. Tale attività può essere fatta anche dagli operatori del SI a seguito di istruzioni dettagliate al fine di avere una migliore organizzazione complessiva.
Ogni utilizzatore che abbia accesso ai dati personali non può trattare i dati se non è stato preventivamente autorizzato ed istruito in tal senso dal Responsabile del trattamento.
I Responsabili delle Aree e dei servizi, comunicano tempestivamente al SI i nominativi degli utilizzatori che devono essere disabilitati e/o le funzioni che devono essere modificate in seguito alla cessazione o mutazione del rapporto lavorativo o istituzionale o variazione di pianta organica.

Art. 17 Gestione dei registri degli accessi

L’accesso ai sistemi, le operazioni di navigazione vengono registrati nei log (registri) di sistema che sono conservati in base alle normative vigenti per 90 giorni.
Tali log non possono essere utilizzati per un controllo sul singolo utilizzatore da parte degli operatori del SI, ma possono essere utilizzati per statistiche generali finalizzate per consultazione al miglior funzionamento complessivo del sistema. I log di sistema sono disponibili per le richieste dell’autorità giudiziaria. Le verifiche del caso vengono effettuate anche qualora si ravvisino situazioni di pericolo per il sistema.

Art. 18 Tutela della Privacy

Ogni operazione di trattamento dei dati da parte dell'operatore avviene solo tramite l'accesso ad archivi attinenti al proprio lavoro, nel rispetto della normativa vigente in materia di privacy e alle indicazioni del Titolare dei dati e del coordinatore interno relativo al proprio servizio, che darà le opportune disposizioni. Si richiede particolare precauzione nelle memorizzazione di informazioni contenenti dati personali e/o sensibili e nell’uso di cartelle ad accesso condiviso.

Parte II – Aspetti organizzativi ed economici

Art. 19 Architettura complessiva dei sistemi informativi

L’architettura tecnologica dei sistemi informativi è definita da SI in base agli indirizzi degli organi politici ed alle necessità tecniche.
La Provincia di Modena favorisce l’utilizzo di formati aperti anche nei rapporti con i cittadini e, dove tecnicamente possibile e conveniente, la diffusione di sistemi open source e il riuso del software
Il SI ha come indirizzo l’installazione centralizzata dei software sul DATA CENTER dell’Ente e l’utilizzo di postazioni di lavoro il più possibile semplificate.
Al fine di razionalizzare i costi e gli spazi, nonché per una migliore organizzazione, sono preferibili stampanti di rete per uffici e gruppi di lavoro omogenei; l’utilizzo di stampanti direttamente connesse alla postazione di lavoro è utilizzato solo per reali particolari necessità.
Nell'utilizzo delle stampanti e dei materiali di consumo in genere (carta, toner, supporti digitali) devono essere evitati in ogni modo sprechi e utilizzi impropri.

Art. 20 Acquisizione di nuovi sistemi informativi
L'acquisto di nuovi software deve essere effettuato seguendo principi di omogeneizzazione e standardizzazione, al fine di mantenere omogeneità tecnologica, verificare la compatibilità tecnica e contenere la spesa corrente inerente i contratti di manutenzione, con esclusione di acquisti inderogabili dovuti ad adeguamenti normativi.

Art. 21 Comitato Servizio Informatico
Il Comitato SI è il tavolo composto dal Responsabile della u.o. Informatica, sistemi e reti, dal Responsabile della u.o. Analisi, programmazione, sistemi gestionali (Responsabile SI), dal Responsabile della u.o. Semplificazione e dematerializzazione e dal Responsabile per la transizione digitale della Provincia (Direttore dell'Area amministrativa).
L'obiettivo del Comitato è quello di evidenziare le priorità di sviluppo dei sistemi informativi e monitorare le attività in corso, concordare regole e azioni comuni ed omogenee.
Il Comitato viene convocato almeno una volta all'anno dal Responsabile della u.o. Informatica, sistemi e reti e dal Direttore dell'Area Amministrativa. Il Comitato può essere convocato anche su richiesta di uno dei componenti.

Parte III - Disposizioni finali e transitorie

Art. 22 Modalità di diffusione del presente documento
Il presente documento viene portato a conoscenza di tutti i dipendenti ed utilizzatori dei sistemi informativi, e rimarrà pubblicato in modo definitivo sul sito della Provincia, insieme ad eventuali modifiche.
Verrà anche presentato direttamente agli operatori in modo da renderli edotti relativamente ai passaggi più tecnici e alle motivazioni da cui è scaturito.
Nel rispetto e nei limiti del presente documento, ulteriori elementi di dettaglio potranno essere emanati dal Responsabile del SI.