COMUNE DI POGGIO MIRTETO

Provincia di Rieti

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

==========

Regolamento per la sicurezza del sistema informatico del comune di Poggio Mirteto.

COMUNE DI POGGIO MIRTETO

Provincia di Rieti

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

==========

COMUNE DI POGGIO MIRTETO

Provincia di Rieti

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

==========

1 Definizione del regolamento di sicurezza della rete informatica

1.1. La rete comunale.

La rete comunale è costituita:

- dalla rete di collegamento telematico tra tutte le varie sedi comunali.
- dai servizi di gestione della rete;
- dai servizi applicativi di base forniti sulla rete, quali Posta, News, Proxy, Web;
- dal servizio di accesso remoto via linee commutate o via tunnel VPN;
- da tutti quegli strumenti di interoperabilità e apparati attivi di rete che permettono ai soggetti autorizzati di accedere alla rete e di comunicare tra loro.

1.2. Protocolli consentiti.

Nella rete comunale viene garantito il supporto per la suite di protocolli TCP/IP, le strutture possono utilizzare al loro interno anche altri protocolli, dandone comunicazione preventiva al gestore della rete, a patto che essi rimangano totalmente confinati all'intero delle struttura comunale.
L'amministrazione comunale favorisce l'utilizzo di applicazioni di tipo "web application" che risultino quindi indipendenti dal sistema operativo installato sui client. Le applicazioni di tipo proprietario verranno gradatamente sostituite concordando la tempistica di sostituzione con le software house licenziatarie delle suddette applicazioni.

1.3. Elenco dei soggetti che possono accedere alla rete.

La rete viene fornita alle strutture comunali e agli Enti e Organizzazioni esplicitamente autorizzate dall'amministrazione comunale.
L'accesso alla rete è consentito solo agli impiegati comunali o ad altri soggetti esplicitamente autorizzati.

1.4. Accesso alla rete via linee commutate.

L'utilizzo di modem installati direttamente sui PC utente facenti parte della rete comunale contattabili dall'esterno della rete è vietato, a meno di casi particolari relativi a specifiche esigenze, che devono essere concordati con il gestore della rete. Qualora un settore intenda intraprendere soluzioni autonome per la fornitura di accesso remoto, deve darne preventiva comunicazione al gestore della rete, garantendo l'adozione di tutte le misure di sicurezza atte a prevenire intrusioni e/o utilizzi illeciti attraverso linea commutata. L'attività può essere intrapresa solo a seguito del riconoscimento da parte del gestore della rete dell'idoneità delle misure di sicurezza adottate.

1.5. Le reti wireless.

L'implementazione di una rete via radio (wireless) comporta a tutti gli effetti un'estensione della rete comunale, e risulta quindi soggetta a tutte le regole stabilite per la rete comunale. In particolare non è consentito implementare in proprio un tale tipo di rete senza l'intervento del gestore della rete. Queste reti devono essere progettate e realizzate dal gestore della rete in accordo con il settore che ne ha fatto richiesta o per la quale questo tipo di tecnologia è stata ritenuta più idonea dal gestore della rete per soddisfare particolari esigenze ambientali o di mobilità. L'utilizzo delle reti wireless deve essere giustificato da una effettiva esigenza che richieda questo tipo di soluzione, in ragione degli inconvenienti che tale scelta

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

comporta. Per quanto riguarda la sicurezza, l'implementazione della soluzione wireless deve essere tale da garantire l'accesso soltanto agli utenti abilitati (autenticazione) e deve prevedere la crittazione del traffico (riservatezza), per portare il livello di sicurezza di questo tipo di reti allo stesso livello garantito da quelle cablate.

1.6. Assegnazione degli indirizzi IP.

Gli indirizzi IP per gli host all'interno della rete comunale vengono assegnati dal gestore della rete, in modo statico. Il piano di indirizzamento IP della rete comunale è amministrato dal gestore della rete.

1.7. Identificazione dei soggetti in rete

Tutti gli utenti a cui vengono forniti accessi alla rete comunale devono essere riconosciuti ed identificabili è vietata l'assegnazione di password collettive o non riconducibili ad un singolo soggetto fisico.

1.8. Inserimento in rete di un host.

Per inserire un host nella rete comunale è necessario:
• Richiedere un indirizzo IP al gestore della rete.
• Installare una protezione antivirus per i sistemi operativi che lo necessitino.
• Controllare se la macchina offre servizi di rete e in caso affermativo eliminarli tutti.
• Applicare tempestivamente tutte le patches di sicurezza del sistema e degli applicativi di cui si intende fare uso e mantenerne nel tempo l'aggiornamento.
La persona a cui la macchina in rete è data in consegna è ritenuta responsabile per quella macchina e per la sua attività nella rete comunale.

1.9. Provvedimenti verso i trasgressori.

In caso di accertata inosservanza delle norme di utilizzo della rete, il gestore della rete prenderà le opportune misure necessarie al ripristino del corretto funzionamento della rete, compresa la sospensione dell'accesso alla rete stessa da parte del trasgressore per motivi cautelari. In caso di reiterata inosservanza, per colpa grave o dolo, il trasgressore sarà suscettibile di provvedimento disciplinare secondo la normativa vigente. In caso di misure d'emergenza, tese a salvaguardare il funzionamento della rete nel suo insieme o in una delle sue parti, il gestore della rete può, come misura transitoria, attuare una sospensione parziale o totale all'accesso alla rete di un singolo client, oppure di uno o più servizi di rete o effettuare una riduzione anche drastica nella banda assegnata a una certo settore.

1.10. Distribuzione delle norme di utilizzo della rete

A tutti gli utenti della rete comunale deve essere distribuito un documento contenente le norme di utilizzo della rete che renda noti per sommi capi i contenuti del regolamento di sicurezza nei riguardi dei comportamenti da tenere nell'uso della rete e dei servizi comunali.

COMUNE DI POGGIO MIRTETO

Provincia di Rieti

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

==========

2 Definizione del regolamento di sicurezza per i servizi e i server.

I server che erogano in rete un servizio informatico devono uniformarsi alle particolari direttive di sicurezza e continuità del servizio descritte di seguito.
In particolare le direttive per questi server riguardano:

- Regole generali per l'amministrazione comunale
- Regole generali per il gestore della rete
- Sicurezza fisica di base dei sistemi
- Sicurezza logica di base dei sistemi
- Gestione degli account per l'accesso ai sistemi
- Protezione da virus informatici
- Interventi sui sistemi da parte di personale esterno

I servizi ufficiali erogati dal comune devono uniformarsi al regolamento descritto nel seguito. In particolare le direttive per questa tipologia di servizi riguardano:

- Privilegi dei servizi
- Aggiornamenti
- Gestione delle password
- Accessi ai servizi
- Logs e loro controllo
- Statistiche sui servizi offerti

2.1 Regole Generali per l'amministrazione comunale.

L'amministrazione comunale deve nominare un responsabile per il sistema informatico con il compito di:

- svolgere un'attività di supervisione e coordinamento tra l'amministrazione comunale e il gestore della rete;
- costituire l'interfaccia ufficiale dell'amministrazione comunale nei confronti dei soggetti che erogano servizi all'amministrazione comunale stessa.

2.2 Regole Generali per il Gestore della rete.

Criteri Generali

Gli amministratori di sistema devono garantire l'efficiente fruibilità del servizio minimizzando il rischio di usi impropri.
Essi devono garantire, per quanto possibile, la disponibilità del servizio secondo i tempi e i modi previsti nel contratto di gestione e manutenzione e operare in modo da minimizzare il rischio di:

- accessi non autorizzati al sistema;
- accessi non autorizzati ai dati;
- usi impropri del sistema che possano arrecare danno ad altri utenti del sistema,
- usi impropri del sistema ovvero non attinenti alle attività istituzionali o comunque estranei alle finalità del trattamento dei dati, anche da parte degli utenti autorizzati.

COMUNE DI POGGIO MIRTETO

Provincia di Rieti

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

==========

2.3 Sicurezza Fisica di Base dei Sistemi

Al fine di proteggere i sistemi, i locali che li ospitano dovranno possedere alcune caratteristiche indipendenti dal tipo di piattaforme hardware e dai sistemi operativi adottati.
Più precisamente, è opportuno che tali locali siano:

- dedicati ai server e preferibilmente presidiati;
- dotati di un sistema, meccanico o elettronico, di selezione degli accessi;
- dotati di un sistema di estinzione degli incendi;
- equipaggiati con dispositivi di stabilizzazione e continuità della tensione;
- climatizzati.

Eventuali interventi di qualsiasi natura (anche non informatica) in tali locali devono sempre avvenire in presenza di personale autorizzato.
In aggiunta a queste misure è consigliabile l'adozione di ulteriori accorgimenti per la restrizione degli accessi da implementare direttamente sui server, tra cui:

- il settaggio del BIOS in modo tale che l'avvio del sistema possa avvenire esclusivamente dal disco rigido di sistema.

2.4 Sicurezza Logica di Base dei Sistemi

Gli amministratori di sistema dovranno prevedere alcuni meccanismi per la sicurezza logica dei server che consentano di ridurre il rischio di esposizione dei dati e di accessi indesiderati ai server.

2.5 Gestione degli Account per l'Accesso ai Sistemi

Gli amministratori devono assegnare a ciascun utente una userid personale per l'accesso ai sistemi: una stessa userid non può essere assegnata a persone diverse neanche in tempi diversi, con l'eccezione delle userid di amministrazione se i sistemi operativi usati ammettono un solo livello di userid per l'amministrazione.
Gli accessi degli amministratori devono comunque avvenire in prima istanza con la userid personale per consentire la tracciabilità delle sessioni.
Gli amministratori devono prontamente disattivare le userid degli utenti se questi perdono il diritto di accesso ai sistemi o se le userid rimangono inutilizzate per più di sei mesi.
Le password di amministrazione dei sistemi dovranno essere:

- cambiate spesso
- note esclusivamente agli amministratori
- diverse per ciascun sistema
- diverse da quelle già utilizzate in passato
- non coincidenti con le userid di amministrazione, neanche temporaneamente
- non banali e comunque di complessità adeguata al tipo di sistema
- non usate per scopi diversi dall'amministrazione dei sistemi

Si presti particolare attenzione a che nessun applicativo faccia uso delle password di amministrazione, nè abbia bisogno dei privilegi di amministratore per il corretto funzionamento.

COMUNE DI POGGIO MIRTETO

Provincia di Rieti

Cap. 02047 e-mail settoreprimo@libero.it
C.F. e P. IVA 00094100575 Fax 0765/22350
C.C.P. 15026024 Tel. 0765/4051

==========

2.6 Protezione da Virus Informatici

I sistemi che ne necessitano devono essere dotati di applicazioni per la difesa da parte di virus informatici, worm, trojan e, in generale, codice indesiderato e dannoso.

Tali applicazioni dovranno avere, di preferenza, la possibilità di controllare i file in tempo reale e di notificare automaticamente la presenza di un virus nel sistema.

Le applicazioni antivirus dovranno essere aggiornate in maniera automatica su base periodica; dovranno inoltre consentire la possibilità di aggiornamento manuale per far fronte ai casi di emergenza, per esempio in seguito a segnalazioni di diffusione di virus importanti.

2.7 Interventi sui Sistemi da Parte di Personale Esterno

Gli accessi ai sistemi da parte di personale esterno, fornitori di hardware o di servizi, dovranno avvenire sotto la supervisione del responsabile per il sistema informatico.

Qualora si rendesse necessario comunicare una o più password di amministrazione, di sistema o di base dati, le stesse dovranno essere sostituite prima e dopo il periodo di utilizzo in modo da svincolarle da un'eventuale logica di assegnazione adottata.