



14 settembre 2026 (RM 1302/2026)

**MM 12/2026 inerente l'adozione del Regolamento concernente la sicurezza delle informazioni**

|          |                                                                                   |          |
|----------|-----------------------------------------------------------------------------------|----------|
| <b>1</b> | <b>Retrospettiva .....</b>                                                        | <b>2</b> |
| <b>2</b> | <b>Misure attuate .....</b>                                                       | <b>3</b> |
| <b>3</b> | <b>Regolamento concernente la sicurezza delle informazioni (RSi) .....</b>        | <b>3</b> |
| 3.1      | Art. 1, Scopo .....                                                               | 4        |
| 3.2      | Art. 2, Applicabilità .....                                                       | 4        |
| 3.3      | Art. 3, Definizione .....                                                         | 4        |
| 3.4      | Art. 4, Responsabilità del Municipio .....                                        | 4        |
| 3.5      | Art. 5, Governance .....                                                          | 4        |
| 3.6      | Art. 6, Obbligo degli assoggettati .....                                          | 4        |
| 3.7      | Art. 7, Accesso degli assoggettati alle informazioni e ai mezzi informatici ..... | 4        |
| 3.8      | Art. 8, Utilizzo dei mezzi informatici .....                                      | 5        |
| 3.9      | Art. 9, Utilizzo dei mezzi informatici - deroga .....                             | 5        |
| 3.10     | Art. 10, Stoccaggio dati .....                                                    | 5        |
| 3.11     | Art. 11, Backup e ripristino .....                                                | 5        |
| 3.12     | Art. 12, Cloud .....                                                              | 5        |
| 3.13     | Art. 13, Posta elettronica e messaggistica .....                                  | 5        |
| 3.14     | Art. 14, Lavoro mobile e telelavoro .....                                         | 5        |
| 3.15     | Art. 15, Segnalazione .....                                                       | 5        |
| 3.16     | Art. 16, Indennità .....                                                          | 5        |
| 3.17     | Art. 17, Sanzioni .....                                                           | 5        |
| <b>4</b> | <b>Incidenze finanziarie .....</b>                                                | <b>6</b> |
| <b>5</b> | <b>Conclusioni .....</b>                                                          | <b>6</b> |
| 5.1      | Aspetti procedurali e formali .....                                               | 6        |
| 5.2      | Attribuzione MM .....                                                             | 7        |
| 5.3      | Proposta di decisione .....                                                       | 7        |
| <b>6</b> | <b>Abbreviazioni .....</b>                                                        | <b>8</b> |
| <b>7</b> | <b>Regolamento concernente la sicurezza delle informazioni (RSi) .....</b>        | <b>9</b> |

Gentile signora Presidente  
Gentile signore ed egregi signori Consiglieri comunali

Vi sottoponiamo l'adozione del Regolamento concernente la sicurezza delle informazioni.

## **1        Retrospettiva**

Il Consiglio comunale in data 23.03.2016 approvava il MM 1/2016 concernente il credito di CHF 67'000.— da destinare all'ammodernamento della rete e delle apparecchiature informatiche.

Con la realizzazione e implementazione dell'infrastruttura di rete informatica moderna, progettata per rispondere alle esigenze operative e tecnologiche dell'organizzazione e per garantire adeguati livelli di connettività, affidabilità e sicurezza. All'epoca della sua realizzazione, l'infrastruttura rappresentava una soluzione adeguata rispetto alle tecnologie disponibili, alle modalità di utilizzo dei sistemi informatici e al livello di rischio associato alle minacce informatiche.

Negli anni successivi essa è stata costantemente ammodernata, applicando il principio di un adeguato rapporto fra investimenti finanziari sostenibili sulla base dei rischi effettivi.

Le minacce informatiche, infatti, non sono statiche, ma si adattano continuamente alle nuove tecnologie e alle modalità di utilizzo dei sistemi. Attacchi di tipo phishing, malware, ransomware, furto di credenziali, accessi non autorizzati e altre forme di compromissione possono rappresentare un rischio concreto per la disponibilità, l'integrità e la riservatezza delle informazioni.

Nell'anno 2025 l'Esecutivo ha commissionato un assesment per la cyber sicurezza con il seguente metodo d'analisi:

1.        identify;
2.        protect;
3.        detect;
4.        respond;
5.        recover.

Per singolo metodo d'analisi si è applicata una "nota" da 0 a 4<sup>1</sup>.

La "nota" dello *stato di destinazione*, il livello di sicurezza futuro che l'organizzazione intende raggiungere mediante l'implementazione di misure tecniche, organizzative e procedurali adeguate, fissata dall'analista era di 2.6.

L'assessment ha permesso di analizzare 160 attività; complessivamente la "nota" ha il punteggio medio di 1.4.

Sottolineiamo il fatto che fino ad ora l'impianto IT comunale ha dato prova di un'adeguata protezione. Negli anni il Comune non ha subito ciberattacchi che hanno compromesso le informazioni stoccate nei server.

## **2 Misure attuate**

Successivamente all'assessment, sono state adottate misure celeri per quelle attività che comportavano rischi cyber accresciuti.

Altre sono state sistemate gradualmente, utilizzando il budget iscritto nei conti di gestione corrente 002.3153.001 e 002.3158.001.

Oltre a quanto già attuato materialmente nell'infrastruttura IT, sono da introdurre, ora, delle IT policy.

Per IT policy s'intende dell'insieme di regole, principi e direttive che stabiliscono come devono essere utilizzati, protetti e gestiti i sistemi informatici, le reti, i dispositivi e i dati di un'organizzazione.

## **3 Regolamento concernente la sicurezza delle informazioni (RSi)**

Fino ad ora le IT policy sono basate sulla direttiva municipale concernente l'utilizzo del sistema informatico, decise nel settembre 2016. Questa disposizione legale non è sufficiente.

Nel nostro ordinamento giuridico dev'essere adottata una base legale formale, adottata dal Legislativo, che codifica la tematica sulla sicurezza delle informazioni.

Con questo impianto normativo, si disporrà di quadro legale sufficiente di carattere genere per gestire formalmente questa attività, coprendo l'intero spettro IT.

La legislazione comunale prevede già alcune disposizioni in questo ambito come gli art. 166 a e 166 b ROC o gli art. 22 a e seguenti del ROD.

---

<sup>1</sup> Classificazione valori:

0, non attuata

1, parzialmente attuata, non definita e approvata completamente

2, parzialmente attuata, definita e approvata completamente

3, attuata, completamente o in gran parte attuata, statica

4, dinamica, attuata, verificata costantemente, migliorata

n/a, inapplicabile/motivo necessario

L'autonomia comunale legislativa residua è data, in quanto né la Confederazione, né il Cantone dispongono di norme che vincolano gli Enti locali.

Abbiamo coinvolto preliminarmente l'incaricato cantonale della protezione dati, per sapere se l'impianto legislativo avesse delle criticità. Benché non sia entrato nel merito, perché è in atto un possibile processo di armonizzazione della fattispecie a livello cantonale, la nostra iniziativa l'ha valutata come meritevole di attenzione.

Successivamente, ma parallelamente all'entrata in vigore del RSi si introdurrà l'Ordinanza comunale d'applicazione del Regolamento concernente la sicurezza delle informazioni, legge materiale che disciplina le questioni tecnico-operative, nonché un adeguamento della diretta municipale concernente l'utilizzo del sistema informatico.

Qui di seguito commentiamo le norme che s'intendono introdurre.

### **3.1 Art. 1, Scopo**

Sono indicati gli scopi che il RSi dovrà perseguire.

Oltre a ciò, funge da norma generale comunale, laddove altre disposizioni analoghe sia di rango superiore o speciale comunale non dispongano altrimenti.

### **3.2 Art. 2, Applicabilità**

Sono indicati esplicitamente gli assoggettati al RSi, ossia gli organi del Comune e i funzionari.

Invece il concetto legale dell'art. 2 cpv 1 let. e) è quello di assoggettare ai vincoli RSi anche i fornitori di prestazioni IT.

### **3.3 Art. 3, Definizione**

Si è descritto l'accezione di definizione nel quale il RSi sarà applicato.

### **3.4 Art. 4, Responsabilità del Municipio**

Si è codificato i compiti che il Municipio dovrà disciplinare mediante ordinanza (ORSi).

### **3.5 Art. 5, Governance**

Tale principio impone ai responsabili della sicurezza delle informazioni, che operano in questo ambito, di redigere un rapporto informativo tecnico indirizzato agli organi politici.

### **3.6 Art. 6, Obbligo degli assoggettati**

Si sono definiti i principi quadro di protezione che gli assoggettati devono improntare durante lo svolgimento della loro funzione.

### **3.7 Art. 7, Accesso degli assoggettati alle informazioni e ai mezzi informatici**

Si sono definiti i principi con i quali gli assoggettati accedano alle informazioni, ai mezzi informatici, ai locali e altre infrastrutture.

### **3.8 Art. 8, Utilizzo dei mezzi informatici**

La norma sancisce l'obbligo d'utilizzo dei mezzi informatici comunali per il trattamento delle informazioni comunali.

### **3.9 Art. 9, Utilizzo dei mezzi informatici - deroga**

Tale norma prevede un'eccezione dell'obbligo di cui all'art. 8, che a seguito di comprovate necessità come: i fornitori di prestazioni di servizio hardware e software, taluni collaboratori, ecc., possono accedere alle informazioni comunali senza un mezzo informatico comunale.

### **3.10 Art. 10, Stoccaggio dati**

Si impone al Comune che i dati siano su server residenti in Svizzera (secondo disposizione sulla Legge della protezione dei dati).

### **3.11 Art. 11, Backup e ripristino**

Si codifica l'obbligo periodico per eseguire queste attività.  
Poi saranno i responsabili della sicurezza di cadenzarle.

### **3.12 Art. 12, Cloud**

L'accesso a queste piattaforme deve beneficiare del nullaosta del Municipio, il quale verifica se tali piattaforme soddisfino i requisiti di protezione dati.

### **3.13 Art. 13, Posta elettronica e messaggistica**

Quale identificazione del mittente va utilizzato il dominio @lavertezzo.ch.  
Tale dominio non può essere utilizzato a scopi privati, perché si vuole evitare un uso improprio.

Una delle eccezioni possibili sono i docenti comunali. Il Cantone mette loro a disposizione il dominio @edu.ti.ch.

### **3.14 Art. 14, Lavoro mobile e telelavoro**

Si è codificato il principio con il quale gli assoggettati, se beneficiano dell'autorizzazione dal Municipio per svolgere la loro funzione con questa modalità lavorativa, come dovranno accedere alla rete comunale.

### **3.15 Art. 15, Segnalazione**

Gli assoggettati hanno l'obbligo di segnalare tempestivamente anomalie al sistema.

Questo permette ai responsabili della sicurezza delle informazioni di essere maggiormente reattivi nell'attuare misure di protezione, nel caso in cui vi siano minacce.

### **3.16 Art. 16, Indennità**

Si stabilisce un indennizzo massimale per l'indennità d'uso di un device privato lavorativi.

Si colma una lacuna legale, che è già applicata.

### **3.17 Art. 17, Sanzioni**

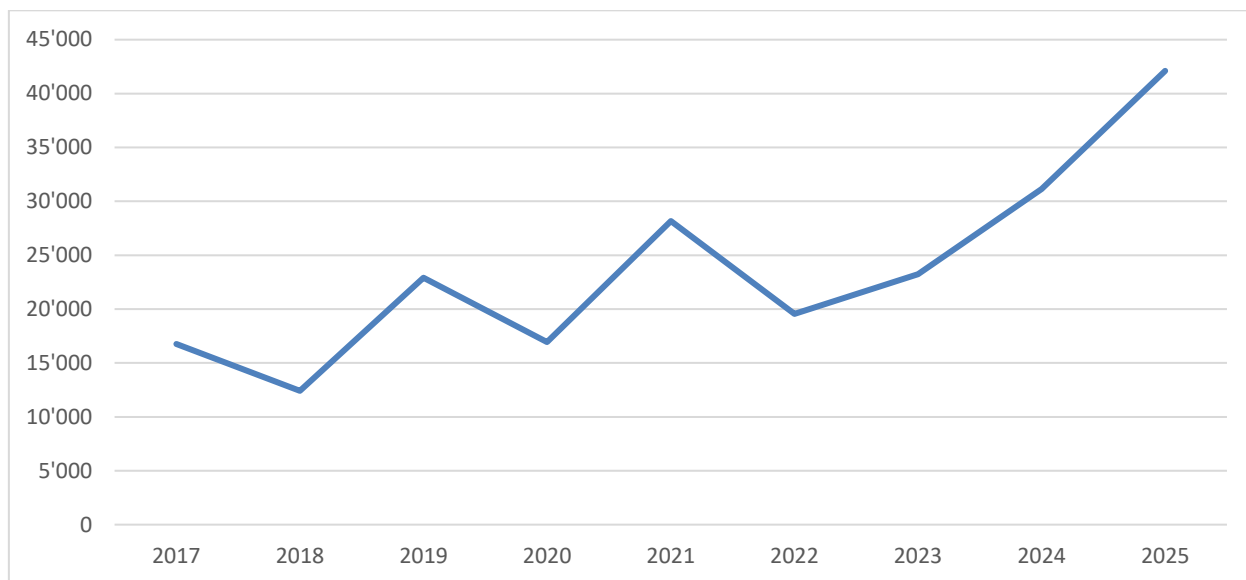
È previsto il sanzionamento nel caso in cui l'assoggettato non si attenga alla disposizione del RSi.

Lo scopo funge da deterrente, perché in caso di violazioni, le conseguenze per il Comune potrebbero essere rilevanti.

#### **4 Incidenze finanziarie**

Di principio le incidenze finanziarie o le richieste di manutenzione sono contenuti nei conti di gestione corrente 002.3153.001 e 002.3158.001 e avallati nei rispettivi preventivi.

L'evoluzione degli anni 2017-2025 è illustrata nel Figura 1.



**Figura 1 – evoluzione investimento IT (hardware e software) anni 2017-2025**

L'evoluzione è in crescendo. Questo trend è influenzato da molteplici fattori come il costo degli hardware generato dal forte sviluppo nell'ambito dell'intelligenza e nei software con canoni mensili o annuali che in precedenza erano una tantum.

#### **5 Conclusioni**

##### **5.1 Aspetti procedurali e formali**

La procedura è disciplinata dall'art. 13 lett. a) LOC, che attribuisce al Consiglio comunale la competenza in materia di regolamenti organici e loro modifiche.

## **5.2 Attribuzione MM**

Richiamati gli artt. 10 RALOC e 47 ROC, si attribuisce alla

### ***Commissione delle petizioni***

l'esame del seguente MM.

La Commissione delle petizioni potrà prendere visione dell'intera documentazione al fine di formulare il necessario rapporto all'indirizzo del Consiglio Comunale (art. 71 e 105 LOC).

Rammentiamo tuttavia che i lavori della Commissione non hanno carattere di pubblicità e i singoli membri sono vincolati all'obbligo di discrezione e riserbo in ossequio alle disposizioni della LOC (in particolare l'art. 104). Pertanto si invita a voler esaminare ed allestire, per iscritto, il rapporto commissionale, il quale dovrà essere depositato, presso la Cancelleria comunale, almeno sette giorni prima della seduta del Consiglio comunale.

La domanda per l'ottenimento della documentazione o della presenza del Capo dicastero ci dovrà pervenire in forma scritta almeno 7 giorni prima della data dei lavori commissionali.

## **5.3 Proposta di decisione**

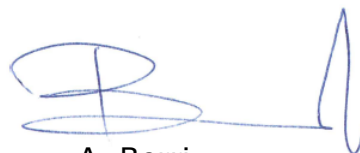
Visto quanto sopra esposto, richiamato l'art. 13 let. a) LOC, il Municipio invita il Consiglio comunale a voler approvare:

1. l'introduzione Regolamento concernente la sicurezza delle informazioni (RSi);
2. l'entrata in vigore della modifica di cui al punto 1 a far data dall'1 gennaio 2027, tramite ordinanza municipale successiva alla ratifica della Sezione enti locali (SEL).

PER IL MUNICIPIO DI LAVERTEZZO

Il Sindaco:

Il Segretario:



A. Berri



D. Gianella

## **6        Abbreviazioni**

|       |                                                           |
|-------|-----------------------------------------------------------|
| AFC   | attestato federale di capacità.                           |
| art.  | articolo/articoli.                                        |
| CFP   | certificato federale di formazione pratica.               |
| cpv   | capoverso/i.                                              |
| let.  | lettera.                                                  |
| LOC   | Legge organica comunale.                                  |
| MM    | messaggio municipale.                                     |
| RALOC | Regolamento d'applicazione della legge organica comunale. |
| RM    | risoluzione municipale.                                   |
| SEL   | Sezione enti locali.                                      |

## **7            Regolamento concernente la sicurezza delle informazioni (RSi)**

### **REGOLAMENTO CONCERNENTE LA SICUREZZA DELLE INFORMAZIONI (RSi)**

Il Consiglio comunale richiamati:

- l'art. 187 LOC;
- l'art. 39 let. t) RALOC;
- l'art. 166 a e 166 b ROC.

risolve

#### **CAPITOLO I DISPOSIZIONI GENERALI**

##### **Scopo**

**Art. 1** <sup>1</sup> Il presente regolamento disciplina il trattamento elettronico delle informazioni per il tramite dei mezzi informatici.

<sup>2</sup> Gli scopi sono:

- a) di definire l'uso lecito, proporzionato e sicuro di reti, dispositivi, applicazioni, dati e servizi digitali del Comune;
- b) di assicurare la riservatezza, l'integrità, la disponibilità, l'autenticità, la tracciabilità e la resilienza delle informazioni;
- c) di prevenire la perdita, il furto, la divulgazione, l'alterazione, la distruzione, l'indisponibilità e il trattamento non autorizzato;
- d) di stabilire la responsabilità, i controlli, la gestione degli incidenti, la continuità e gli obblighi verso le autorità;
- e) di promuovere i comportamenti sicuri, non colpevolizzanti e orientati alla segnalazione tempestiva;
- f) di fronteggiare le cyberminacce.

<sup>3</sup> Sono riservate le norme speciali previste da altre leggi federali, cantonali e comunali.

##### **Applicabilità**

**Art. 2** <sup>1</sup> Al presente regolamento sono assoggettati:

- a) il Consiglio comunale;
- b) il Municipio;
- c) l'Amministrazione comunale, incluso l'Istituto scolastico;
- d) gli utenti terzi che sono coinvolti nel trattamento elettronico delle informazioni per il tramite dei mezzi informatici, secondo il presente regolamento;
- e) i fornitori di prestazioni hardware e software che per le loro commesse interagiscono, anche passivamente, nell'ambito del presente regolamento.

##### **Definizione**

**Art. 3** <sup>1</sup> Ai sensi del presente regolamento s'intende per:

- a) trattamento elettronico delle informazioni: è l'insieme delle attività svolte mediante strumenti elettronici o informatici per raccogliere, registrare, organizzare, elaborare, conservare, consultare, modificare, trasmettere o cancellare informazioni;
- b) mezzi informatici: quelle tecnologie dell'informazione e della comunicazione, segnatamente applicazioni, sistemi d'informazione e collezioni di dati nonché installazioni, prodotti e servizi che servono all'elaborazione elettronica delle informazioni.

<sup>2</sup> Oltre a quanto previsto nell'art. 3 cpv 1 inoltre s'intende per:

- a) attività sensibile sotto il profilo della sicurezza:
  - 1. il trattamento di informazioni;
  - 2. l'amministrazione, l'esercizio, la manutenzione e la verifica di mezzi informatici del livello di sicurezza;

- b) ciberincidente: un evento che si verifica nell'utilizzo di mezzi informatici e che compromette la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento;
- c) ciberattacco: un ciberincidente provocato intenzionalmente;
- d) cyberminaccia: qualsiasi circostanza o evento che ha il potenziale di provocare un ciberincidente;
- e) vulnerabilità: una cyberminaccia riconducibile a punti deboli o errori nei mezzi informatici.

## **CAPITOLO 2**

### **RESPONSABILITÀ, GOVERNANCE E GESTIONE DEL RISCHIO**

#### **Responsabilità del Municipio**

**Art. 4** <sup>1</sup> È responsabile per:

- a) mezzi informatici:
  - 1. di definirne l'architettura;
  - 2. l'acquisizione, l'installazione, la configurazione e l'inventario;
  - 3. l'esercizio, la manutenzione, la sorveglianza e la formazione;
- b) disciplinare la protezione e l'uso sia dei mezzi informatici e del trattamento elettronico delle informazioni.

#### **Governance**

**Art. 5** <sup>1</sup> Il Municipio designa i responsabili della sicurezza delle informazioni e i compiti a loro affidati.

<sup>2</sup> I responsabili della sicurezza delle informazioni elaborano un rapporto all'indirizzo del Municipio, entro il 31 gennaio dell'anno successivo, che analizza l'attività dell'esercizio precedente.

#### **Obbligo degli assoggettati**

**Art. 6** <sup>1</sup> Gli assoggettati secondo l'art. 2, provvedono affinché, conformemente alle rispettive necessità di protezione, le informazioni:

- a) siano accessibili soltanto alle persone autorizzate (confidenzialità);
- b) siano disponibili quando sono necessarie (disponibilità);
- c) non possano essere modificate senza autorizzazione o per inavvertenza (integrità);
- d) siano trattate in maniera documentabile (tracciabilità).

<sup>2</sup> Gli assoggettati secondo l'art. 2, provvedono affinché, conformemente alle rispettive necessità di protezione, i mezzi informatici:

- a) siano protette le credenziali e i dispositivi;
- b) siano segnalati immediatamente gli errori, i messaggi sospetti, la perdita di dispositivi, gli accessi anomali e le divulgazioni;
- c) collaborano alle verifiche e non ostacolano le misure di contenimento;
- d) non siano aggirati i controlli, di disattivare protezioni o svolgere attività illecite, offensive o estranee ai compiti.

#### **Accesso degli assoggettati alle informazioni e ai mezzi informatici**

**Art. 7** <sup>1</sup> Il Municipio provvede affinché gli assoggettati che hanno accesso alle informazioni, ai mezzi informatici, ai locali e alle altre infrastrutture del Comune:

- a) siano identificate in funzione dei rischi;
- b) seguano formazioni continue adeguate al loro livello.

<sup>2</sup> Possono impiegare metodi di verifica biometrici se è necessario per l'identificazione delle persone in funzione dei rischi. I dati biometrici sono distrutti allo scadere dell'autorizzazione d'accesso.

<sup>3</sup> Come identificatore di persone possono inoltre utilizzare sistematicamente il numero AVS di cui all'articolo 50c della legge federale del 20 dicembre 1946 sull'assicurazione per la vecchiaia e per i superstiti.

#### **Utilizzo dei mezzi informatici**

**Art. 8** <sup>1</sup> Gli assoggettati di cui all'art. 2 che per lo svolgimento della loro funzione, sono obbligati di utilizzare i mezzi informatici comunali.

<sup>2</sup> L'utilizzo dei mezzi informatici comunali a scopi privati non è autorizzato.

**Utilizzo dei  
mezzi  
informatici -  
deroghe**

**Art. 9** <sup>1</sup> Il Municipio è competente di rilasciare deroghe all'obbligo di cui all'art. 8.

<sup>2</sup> Le deroghe sono subordinate ai medesimi principi di trattamento elettronico delle informazioni per il tramite dei mezzi informatici sanciti dal presente regolamento.

### **CAPITOLO 3**

#### **PROTEZIONE INFORMATICA E CIBERSICUREZZA**

**Stoccaggio dati**

**Art. 10** <sup>1</sup> Lo stoccaggio dei dati, unitamente dei backup, devono avvenire su server propri residenti in Svizzera.

**Backup e  
ripristino**

**Art. 11** <sup>1</sup> Sono eseguiti periodicamente.

<sup>2</sup> Sono da pianificare ed eseguire test di ripristino periodici, includendo configurazioni, identità e dati.

**Cloud**

**Art. 12** <sup>1</sup> I servizi cloud necessari al trattamento elettronico delle informazioni possono essere utilizzati unicamente con l'autorizzazione del Municipio.

<sup>2</sup> I servizi cloud devono rispettare i principi della protezione dati, unitamente a quelli del presente regolamento.

**Posta  
elettronica e  
messaggistica**

**Art. 13** <sup>1</sup> Gli assoggettati di cui all'art. 2 che per lo svolgimento della loro funzione, utilizzano il dominio @lavertezzo.ch.

<sup>2</sup> L'utilizzo del dominio @lavertezzo.ch a scopi privati non è autorizzato.

<sup>3</sup> Il Municipio può concedere deroghe all'utilizzo di altri domini, subordinandone i medesimi principi di trattamento elettronico delle informazioni per il tramite dei mezzi informatici sanciti dal presente regolamento.

**Lavoro mobile e  
telelavoro**

**Art. 14** <sup>1</sup> Gli assoggettati di cui all'art. 2 che ne hanno la necessità, l'accesso da remoto deve avvenire unicamente per il tramite VPN o MFA approvati dal Municipio.

**Segnalazione**

**Art. 15** <sup>1</sup> Gli assoggettati di cui all'art. 2 rilevano o sospettano un incidente informano immediatamente i responsabili della sicurezza previsti dall'art. 5, anche se hanno commesso un errore o non dispongono di prove complete.

### **CAPITOLO 4**

#### **INDENNITÀ**

**Indennità di  
utilizzo**

**Art. 16** <sup>1</sup> Per gli assoggettati che hanno ottenuto la deroga di cui all'art. 9, può essere riconosciuta un'indennità per l'uso di device privati fino ad un importo massimo di 50 CHF/mensili.

<sup>2</sup> Il Municipio è competente nell'elaborare il catalogo degli indennizzi.

### **CAPITOLO 5**

#### **DISPOSIZIONI FINALI**

**Sanzioni**

**Art. 17** <sup>1</sup> Conformemente all'art. 145 LOC il Municipio punisce con una multa sino a CHF 10'000 le infrazioni al presente regolamento, alle relative ordinanze municipali e direttive.

**Entrata in vigore**

**Art. 18** <sup>1</sup> Il presente regolamento entra in vigore tramite ordinanza municipale dopo l'approvazione della Sezione degli Enti locali.