**PIANO DI PROTEZIONE DEI DATI PERSONALI**

**E GESTIONE DEL RISCHIO DI VIOLAZIONE**

**SINTESI DPIA**

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE**

**DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**

(da esibire su richiesta dell'Autorita' di controllo)

**ALLEGATO N. XX**

|  |  |
| --- | --- |
| Titolo del Documento |  |
| Numero di versione |  |
| Data ultimo aggiornamento | 30/04/2020 |
| Stato del documento | Approvato dal titolare con proprio provvedimento |
| Estensori del documento | - Titolare del trattamento |
| Riferimento per comunicazioni in merito al documento | - Punti di contatto del titolare del trattamento - TTD |
| Modalita' di distribuzione del presente documento e delle eventuali nuove versioni | - Trasmissione tramite la rete intranet  - Conservazione con supporto informatico |

|  |  |
| --- | --- |
| **TIPOLOGIA TRATTAMENTO** | |
| **Denominazione del trattamento** | Scheda n. 65 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi alla verifica della legittimita', del buon andamento e dell'imparzialita' dell'attivita' amministrativa |
| **SETTORE** | AFFARI GENERALI E ISTITUZIONALI |
| **SERVIZIO** | SEGRETERIA GENERALE |
| **UFFICIO:** denominazione e punti di contatto | Segreteria generale |
| **Titolare trattamento:** denominazione e punti di contatto | Comune di VETTO  Sindaco Ruffini Fabio Tel. 0522 815221  Email: sindaco@comune.vetto.re.it |
| **Contitolare/i trattamento:** denominazione e punti di contatto |  |
| **Responsabile trattamento:** denominazione e punti di contatto |  |
| **Sub-Responsabile/Incaricato trattamento:** denominazione e punti di contatto |  |

|  |  |
| --- | --- |
| **VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI** | |
| **Origine dei rischi rilevati dalla prospettiva degli interessati** |  |
| **Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati** |  |
| **Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati** |  |
| **Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati** |  |

|  |  |  |
| --- | --- | --- |
| **MISURE PREVISTE PER AFFRONTARE I RISCHI** | | |
| **Misure tecniche informatiche** | - ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)  - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)  - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)  - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)  - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)  - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)  - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)  - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) |
| **Misure tecniche logistiche** | - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti  - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere |
| **Misure organizzative** | - MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative  - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri  - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti  - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati  - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento  - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante  - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti |
| **Misure procedurali** | - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi  - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione  - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante  - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali  - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico  - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach  - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche  - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP. |

|  |
| --- |
| **ELENCO TRATTAMENTI**  **INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI** |

Consulenza e assistenza del Segretario/Direttore agli organi di indirizzo politico