Allegato C alla deliberazione della Giunta comunale n. 9 di data 27 gennaio 2026
LA PRESIDENTE avv. Arianna Fiorio
IL SEGRETARIO GENERALE dott. Giorgio Osele
Documento informatico firmato digitalmente ai sensi del testo unico D.P.R. 28/12/2000, n. 445, del D. Lgs. 07/03/2005, n. 82 e norme collegate, il quale sostituisce il testo cartaceo e la firma autografa.

# Analisi del rischio sul trattamento WHISTLEBLOWING TRAMITE UTILIZZO DELLA PIATTAFORMA WEB

| | Evento / descrizione del rischio | Minaccia | Impatto (dare un valore da 1 a 5) | Probabilità (dare un valore da 1 a 5) | Indice qualitativo di gravità (risultato automatico) | Note | Documentazione di riferimento (evidenze documentali da personalizzare) | Misure di mitigazione del rischio individuate al fine di abbassare il livello di rischio (da personalizzare) |
|---|---|---|---|---|---|---|---|---|
| 1 | **Uso illecito di credenziali di autenticazione:** possibilità di avere accesso a dati per i quali non si dispone dell'autorizzazione al trattamento | Uso non autorizzato di apparecchiature o software | 3 | 1 | 3 | Il RPCT, presidente dell'OIV e il detentore delle chiavi sono stati autorizzati e istruiti circa l'obbligo di non condividere le credenziali personali o di lasciarle incustodite;<br>le credenziali al presidente dell'OIV/RPCT e al detentore delle chiavi sono state consegnate personalmente;<br>la password dev'essere modificata obbligatoriamente al primo accesso;<br>la password dev'essere forte oltre che criptata (caratteri e password non uguale all'ultima inserita)<br>il cambio password è obbligatorio ogni anno;<br>ad ogni cambio di RPCT, presidente dell'OIV, viene disattivata e riattivata una nuova utenza;<br>norma di riferimento per il corretto comportamento del presidente dell'OIV, RPCT e detentore delle chiavi è il Testo Unico del pubblico impiego oltre a indicazioni specifiche che sono indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente contenute nel PIAO; tali soggetti sono stati autorizzati al trattamento dei dati personali | Misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| | | Innalzamento illecito dei privilegi di accesso da parte dell'amministratore dell'applicativo | 1 | 1 | 1 | nomina al fornitore quale responsabile del trattamento contenente istruzioni circa l'obbligo di non alzare i privilegi di accesso agli utenti della piattaforma | Nomina del fornitore della piattaforma informatica | |
| | | Violazione dei profili di accesso da parte di hackers | 3 | 2 | 6 | la password non viene mai memorizzata in chiaro sulla piattaforma ma vengono memorizzate con un hash costruito da un site randomico a 128 bit e algoritmo Argon 2;<br>sono poste in essere misure di sicurezza del software e di sicurezza della rete che dovrebbero garantire la protezione da attacchi hacker; | Misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| 2 | **Carenza di consapevolezza, disattenzione:** la scarsa consapevolezza nel trattamento dei dati può causarne la diffusione, modifica o perdita | Divulgazione involontaria dei dati | 3 | 3 | 9 | le e-mail ricevute da RPCT, presidente dell'OIV e dal detentore delle chiavi non permettono la lettura della segnalazione, per la quale è necessario accedere all'applicativo. Pertanto, anche se l'e-mail dovesse essere erroneamente divulgata, non sarebbe possibile leggere il contenuto | | |
| | | Affido di trattamenti a personale inesperto o non sufficientemente formato | 2 | 2 | 4 | Il RPCT, presidente dell'OIV e il detentore delle chiavi sono stati autorizzati e istruiti al trattamento dei dati personali. I ruoli sono stati assegnati a figura apicale e all'organo preposto ai controlli;<br>inoltre, tali soggetti devono attenersi alla norma di riferimento per il corretto comportamento, il TU per il pubblico impiego, oltre che alle indicazioni specifiche indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente | | |
| | | Utilizzo di software o servizi senza contratto di manutenzione | 3 | 1 | 3 | la piattaforma è coperta da contratto e il fornitore è stato opportunamente nominato quale responsabile del trattamento | Contratto con fornitore della piattaforma web | |
| | | Vendor lock-in e portabilità dei dati non prevista | 1 | 2 | 2 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo, a richiesta del titolare, di restituire i dati trattati per e in relazione alla cessazione del contratto | Nomina del fornitore della piattaforma informatica | |
| | | Inefficace protezione dei sistemi | 3 | 2 | 6 | il software è protetto dalle misure di sicurezza poste in essere dal fornitore della piattaforma; ulteriori misure di sicurezza sono poste in essere dall'amministratore di sistema dell'Ente | Misure di sicurezza garantite dal fornitore della piattaforma informatica<br>Misure di sicurezza relative alle infrastrutture dell'Ente fornite dall'amministratore di sistema | |
| | **Comportamenti sleali o fraudolenti:** il trattamento effettuato per fini diversi da quelli strettamente necessari all'espletamento del proprio lavoro può provocare furto, cancellazione e modifica dei dati | Uso non autorizzato degli strumenti per scopi personali | 3 | 2 | 6 | Il RPCT, presidente dell'OIV e il detentore delle chiavi sono stati autorizzati e istruiti al trattamento dei dati personali;<br>inoltre, tali soggetti devono attenersi alla norma di riferimento per il corretto comportamento, il Testo Unico del pubblico impiego, oltre che alle indicazioni specifiche indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente contenute nel PIAO; | Atto di nomina a RPCT, presidente dell'OIV e al detentore delle chiavi | |
| | | Stampa, scansione o copia, anche tramite immagini, di documenti e dati | 3 | 2 | 6 | RPCT/OIV e eventuale detentore delle chiavi sono stati autorizzati e istruiti al trattamento dei dati personali;<br>inoltre, tali soggetti devono attenersi alla norma di riferimento per il corretto comportamento, il TU pubblico impiego, oltre che alle indicazioni specifiche indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente contenute nel PIAO;<br>si stima un impatto alto in quanto l'eventuale danno in termini di riservatezza e reputazione di segnalante e segnalato sarebbe alto;<br>nonostante non si siano mai verificati episodi di cattiva gestione delle segnalazioni legati alla minaccia in esame, il titolare ritiene maggiormente tutelante introdurre delle specifiche regole comportamentali al fine di prevenire comportamenti scorretti (anche se involontari) | Atto di nomina a RPCT, presidente dell'OIV e al detentore delle chiavi | ~~adozione del disciplinare~~ delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica Allegato B alla deliberazione della Giunta comunale n. 85 di ~~data 13 giugno 2023~~ |
| | | Visione dello schermo di pc o smartphone da parte di soggetti non autorizzati, della documentazione e dell'ascolto | 2 | 2 | 4 | Il RPCT, presidente dell'OIV e il delle chiavi hanno un ufficio singolo chiuso a chiave; sono stati autorizzati e istruiti al trattamento dei dati personali;<br>inoltre, tali soggetti devono attenersi alla norma di riferimento per il corretto comportamento, il Testo Unico del pubblico impiego, oltre che alle indicazioni specifiche indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente/MOG 231; | Atto di nomina a RPCT, presidente dell'OIV e al detentore delle chiavi | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Falsificazione di documenti contenenti dati personali | 3 | 2 | 6 | Il RPCT, presidente dell'OIV e eventuale detentore delle chiavi sono stati autorizzati e istruiti al trattamento dei dati personali; inoltre, tali soggetti devono attenersi alla norma di riferimento per il corretto comportamento, il TU pubblico impiego, oltre che alle indicazioni specifiche indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente contenute nel PIAO;<br>nel caso specifico, in caso di falsificazione dei documenti da parte di uno dei soggetti abilitati, la veridicità del documento è garantita dal controllo del RPCT | Atto di nomina a RPCT/OIV o eventuale detentore delle chiavi | |
| **4** | **Errori materiali:** un errore umano durante il trattamento può provocare danni come la cancellazione, la modifica, la scrittura errata di dati o la diffusione | Disattenzioni ed errori in fase di utilizzo dei software applicativi | 2 | 2 | 4 | qualora vi fosse un errore umano, la veridicità del documento è garantita dal controllo del RPCT; peraltro, al RPCT, presidente dell'OIV arriva contestualmente l'email di notifica della presenza di una nuova segnalazione (in caso di cancellazione accidentale) | | |
| | | Copia dei dati su supporti non sicuri | 2 | 3 | 6 | Il RPCT, presidente dell'DV e al detentore delle chiavi sono stati autorizzati e istruiti al trattamento dei dati personali;<br>inoltre, tali soggetti devono attenersi alla norma di riferimento per il corretto comportamento, il TU pubblico impiego, oltre che alle indicazioni specifiche indicate da ANAC nelle Linee guida sul whistleblowing e delle misure anticorruzione dell'Ente contenute nel PIAO;<br>nonostante non si siano mai verificati episodi di cattiva gestione delle segnalazioni legati alla minaccia in esame, il titolare ritiene maggiormente tutelante introdurre delle specifiche regole comportamentali al fine di prevenire comportamenti scorretti (anche se involontari);<br>Normalmente non sono utilizzati supporti esterni (es. usb, hard disk esterni), si ritiene comunque opportuno introdurre delle regole specifiche nel caso in cui si ponga il problema | | adozione del disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica Allegato B alla deliberazione della Giunta comunale n. 85 di data 13 giugno 2023 |
| | | Salvataggio di backup delle banche dati non previsto o non sicuro | 2 | 1 | 2 | il fornitore della piattaforma si occupa del backup e garantisce di poter ripristinare entro le 24 ore dalla criticità la disponibilità del dato | Misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| | | Conservazione dei dati più a lungo del necessario | 2 | 2 | 4 | la conservazione è prevista, come indicato nelle FAQ ANAC, per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; sarà quindi premura del RPCT, presidente dell'OIV, cancellare i dati conservati e non più necessari. Peraltro, il D. lgs. 24/2023 prevede un termine massimo di conservazione di 5 anni | | |
| **5** | **Azione di virus informatici o di codici malefici**: l'azione di virus o codice malefico può provocare la perdita dei dati, così come il blocco del sistema con la conseguente inaccessibilità ai dati stessi oppure la modifica all'integrità e correttezza degli stessi | Infezioni da virus/malware o altro codice malevolo | 2 | 1 | 2 | il software è protetto dalle misure di sicurezza poste in essere dal fornitore della piattaforma; ulteriori misure di sicurezza sono poste in essere dall'amministratore di sistema dell'Ente; formazione interna sulla sicurezza informatica e le principali minacce; | Misure di sicurezza garantite dal fornitore della piattaforma informatica Misure di sicurezza relative alle infrastrutture dell'Ente fornite dall'amministratore di sistema | |
| | | Attacchi di tipo phishing (e-mail) | 4 | 1 | 4 | formazione interna sulla sicurezza informatica e le principali minacce | | |
| **6** | **Malfunzionamento, indisponibilità o degrado degli strumenti:** il blocco del server può provocare il blocco dell'accesso ai dati e la conseguente impossibilità di effettuare i trattamenti degli stessi | Sovraccarico della capacità di elaborazione | 3 | 2 | 6 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo di garantire buone performance del servizio | Nomina del fornitore della piattaforma informatica | |
| | | Dispositivi di memorizzazione saturi | 3 | 1 | 3 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo di garantire buone performance del servizio | Nomina del fornitore della piattaforma informatica | |
| | | Anomalie e malfunzionamento del software | 3 | 2 | 6 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo di garantire buone performance del servizio e aggiornare il sistema o intervenire prontamente per risolvere eventuali problematiche | Misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| | | Invecchiamento delle apparecchiature server | 3 | 1 | 3 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo di garantire buone performance del servizio | Nomina del fornitore della piattaforma informatica | |
| | | Problemi con il backup delle banche dati | 3 | 2 | 6 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo di garantire buone performance del servizio anche garantendo il funzionamento di un sistema di backup | Nomina del fornitore della piattaforma informatica e misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| **7** | **Inadeguatezza degli strumenti:** l'utilizzo di strumenti inadeguati può causare la perdita dei dati e il trattamento illecito degli stessi | Utilizzo di software soggetto a vulnerabilità | 2 | 2 | 4 | nella nomina al responsabile del trattamento è stato disciplinato l'obbligo di garantire buone performance del servizio | Nomina del fornitore della piattaforma informatica e misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| **8** | **Problemi di accesso o intercettazione delle informazioni in rete:** l'impossibilità di accedere ai servizi di rete può causare l'indisponibilità dei dati; l'intercettazione delle informazioni in rete può consentire l'accesso a dati di cui non si è autorizzati al trattamento | Trasmissioni di dati in maniera non sicura | 3 | 2 | 6 | la comunicazione avviene tramite software protetto che viene sottoposto periodicamente a penetration test e vulnerability assesment;<br>la maggior parte dei potenziali segnalanti lavora in TelPAT che è rete protetta | Nomina del fornitore della piattaforma informatica e misure di sicurezza garantite dal fornitore della piattaforma informatica | |
| | | Perdita della connessione di rete | 4 | 2 | 8 | può capitare ma il problema non è rilevante tanto da ostacolare l'effettuazione della segnalazione che possono essere effettuate tramite altro strumento | | |
| | | Connettività insufficiente | 4 | 2 | 8 | può capitare ma il problema non è rilevante tanto da ostacolare l'effettuazione della segnalazione che possono essere effettuate tramite altro strumento | | Installazione di FO |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **9** | **Asportazione o furto di strumenti contenenti dati:** i supporti di memorizzazione contenenti dati possono essere rubati causandone la perdita e la diffusione non autorizzata | Furto di dispositivi o documenti | 3 | 2 | 6 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore;<br>l'eventuale gestionale documentale dell'attività di trattamento viene effettuata solo dal gestione della segnalazione da parte del RPCT, presidente dell'OIV, che è stato autorizzato e istruito al corretto trattamento dei dati e che deve seguire le norme previste dal codice di comportamento,<br>smartphone protetti da password di sblocco;<br>si ritiene comunque opportuno introdurre delle regole specifiche nel caso in cui si ponga il problema; | nomina a RPCT, presidente dell'OIV<br>codice di comportamento | adozione del disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica<br>Allegato B alla deliberazione della Giunta comunale n. 85 di data 13 giugno 2023 |
| | | Accesso a dati archiviati su supporti di memorizzazione di massa | 3 | 1 | 3 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore;<br>l'eventuale gestione documentale dell'attività di trattamento viene effettuata solo dal gestione della segnalazione da parte del RPCT presidente OIV, che è stato autorizzato e istruito al corretto trattamento dei dati e che deve seguire le norme previste dal codice etico e di condotta dal codice di comportamento;<br>smartphone protetti da password di sblocco;<br>si ritiene comunque opportuno introdurre delle regole specifiche nel caso in cui si ponga il problema;<br>si stima un impatto alto in quanto l'eventuale danno in termini di riservatezza e reputazione sarebbe alto | nomina RPCT e OIV<br>codice di comportamento | adozione del disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica<br>Allegato B alla deliberazione della Giunta comunale n. 85 di data 13 giugno 2023 |
| **10** | **Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria:** la distruzione delle apparecchiature o dei locali può provocare la perdita dei dati nonché l'impossibilità fisica di riprendere il servizio | Eventi naturali calamitosi (terremoto, inondazione, incendio) | 3 | 1 | 3 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore; pertanto il problema, nel caso di utilizzo di piattaforma informatica, non si presenta<br>nel caso di modalità cartacea, l'ente ha adottato misure di sicurezza fisiche al fine di garantire la sicurezza dei documenti cartacei;<br>si ritiene comunque opportuno introdurre delle regole specifiche nel caso in cui si ponga il problema; | Nomina del fornitore della piattaforma informatica e misure di sicurezza garantite dal fornitore della piattaforma informatica | adozione del disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica |
| | | Atti vandalici | 2 | 1 | 2 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore; pertanto il problema, nel caso di utilizzo di piattaforma informatica, non si presenta<br>si ritiene comunque opportuno introdurre delle regole specifiche nel caso in cui si ponga il problema; | Nomina del fornitore della piattaforma informatica e misure di sicurezza garantite dal fornitore della piattaforma informatica | adozione del disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica |
| **11** | **Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...):** un guasto può comportare la corruzione dei dati così come il blocco del servizio di trattamento erogato | Interruzione di corrente e sbalzi di tensione/cortocircuito | 3 | 1 | 3 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore;<br>è presente un gruppo di continuità funzionante | Nomina dell'amministratore di sistema<br>Nomina del fornitore della piattaforma informatica e misure di sicurezza garantite dal fornitore della piattaforma informatica; | |
| **12** | **Errori umani nella gestione della sicurezza fisica:** l'errore può comportare guasti e/o la compromissione delle contromisure adottate | Smarrimento di un dispositivo di memorizzazione elettronico | 3 | 1 | 3 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore;<br>l'eventuale gestione documentale dell'attività di trattamento viene effettuata solo dal gestore della segnalazione da parte del RPCT, presidente dell'OIV, che è stato autorizzato e istruito al corretto trattamento dei dati e che deve seguire le norme previste dal codice di comportamento;<br>smartphone protetti da password di sblocco; | Nomina a RPCT, presidente dell'OIV<br>codice di comportamento | adozione del disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica |
| | | Errori o incuria nello scarto o nella stampa dei documenti | 2 | 2 | 4 | il software è interamente web-based e non necessità l'installazione di alcun componente sul client dell'utilizzatore;<br>l'eventuale gestione documentale dell'attività di trattamento viene effettuata solo dal gestore della segnalazione da parte del RPCT, presidente dell'OIV che è stato autorizzato e istruito al corretto trattamento dei dati e che deve seguire le norme previste dal codice di comportamento;<br>smartphone protetti da password di sblocco; | nomina a RPCT, presidente dell'OIV<br>codice di comportamento | delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica<br>Allegato B alla deliberazione della Giunta comunale n. 85 di |
| **13** | **Problemi di tipo organizzativo:** eventuali criticità di tipo organizzativo possono influenzare le modalità di trattamento adottate dal personale | Stress per carichi di lavoro troppo elevati | 3 | 1 | 3 | il RPCT lavora in un sistema organizzato e compartimentalizzato tale per cui le funzioni sono distribuite su diversi uffici/servizi; l'OIV è un organismo appositamente incaricato della funzione | | |
| | | Indisponibilità (malattia, sciopero, pensionamento, riassegnazione, licenziamento) | 2 | 1 | 2 | Pertanto, in caso di impedimento o cessazione della funzione, è prevista dalla legge la nomina di un nuovo RPCT, presidente dell'OIV, da parte dell'organo di governo. In caso di assenza temporanea di RPCT la segnalazione può essere gestita dall'altro soggetto con funzioni vicarie di Vice Segretario essendo l'RPCT il Segretrio generale. | | |
| | | Pressioni esterne (corruzione, ricatto, cerchia familiare) | 3 | 1 | 3 | ci possono essere due tipi di pressioni esterne: nei confronti del segnalante o nei confronti dei controllori (RPCT, presidente dell'OIV) o del detentore delle chiavi. La veridicità della segnalazione verrà valutata da chi riceve la segnalazione. | codice di comportamento | |