RISK ASSESSMENT AND SECURITY MEASURE FOR PERSONAL DATA PROCESSING

Assessment of the level of risk for processing operation **Didattica a distanza** and a proposal for appropriate technical and organizational security measures.

Section I – Definition and Context of the Processing Operation

PROCESSING OPERATION DESCRIPTION	ANSWER	
Personal Data Processed	Domenico Portale	
Processing Purpose	Svolgimento di attività didattiche consistenti in lezioni preregistrate e/o in diretta, assegnazione compiti, annotazione assenze e valutazioni.	
Data Subject	Alunni	
Processing Means	Utilizzo della piattaforma G-suite nella sue applicazioni Google Classroom, Drive, Hangouts Meet, sezione compiti del registro elettronico adottato dalla scuola.	
Recipients of Personal Data	Internal	Docenti degli alunni
	External	
Data Processor Used	Dirigente Scolastico	

Section II – Evaluation of the Impact

Confidentiality impact assessment: **Low**

Non utilizzo di materiale cartaceo e non è previsto trasporto laptop con dati personali. I dati non possono essere inviati a destinatari non autorizzati

Integrity impact assessment: **Low**

Nessun record necessario può essere modifcato.

Availability impact assessment: **Low**

Nessuno dei casi descritti può verificarsi

IMPACT ASSESSMENT		
Confidentiality	**Integrity**	**Availability**
Low	Low	Low
	Overall Impact Evaluation	Low

Section III – Analysis of the Threats per Assessment Area

Network and Technical Resources threat probability: Low

- **Is any part of the processing of personal data performed through the internet? No**
- **Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)? No**
- **Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service? No**
- **Can unauthorized individuals easily access the data processing environment? No**
- **Is the personal data processing system designed, implemented or maintained without following relevant documented best practices? No**

Processes/Procedures related to the processing of personal data threat probability: Low

- **Are the roles and responsibilities with regard to personal data processing vague or not clearly defined? No**
- **Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined? No**
- **Are the employees allowed to bring and use their own devices to connect to the personal data processing system? Yes**
  Docenti e alunni, se autorizzati, accedono con strumentazioni proprie.
- **Can personal data processing activities be performed without log files being created? No**

Parties/People involved in the processing of personal data threat probability: Low

- **Is the processing of personal data performed by an undefined number of employees? No**
- **Is any part of the data processing operation performed by a contractor/third party (data processor)? No**
- **Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated? No**
- **Is the personnel involved in the processing of personal data unfamiliar with security matters? No**
- **Do the persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data? No**

Business sector and scale of processing threat probability: Low

ASSESSMENT AREA	PROBABILITY	
Network and Technical Resources	Low	1
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Low	1
Overall Threat Occurrence Probability	Low (4)	

Section IV – Evaluation of Risk

	IMPACT LEVEL			
THREAT OCCURRENCE PROBABILITY		Low	Medium	High / Very High
	Low	X		
	Medium			
	High			

Section V – Organizational Security Measures

It should be noted that the adequacy of measures to specific risk levels should not be perceived as absolute. Va notato che l'adeguatezza delle misure a livelli di rischio specifici non deve essere percepita come assoluta. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk. A seconda del contesto del trattamento dei dati personali, l'organizzazione può prendere in considerazione l'adozione di misure aggiuntive, anche se assegnate a un livello di rischio più elevato. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive or the NIS Directive. Inoltre, l'elenco proposto di misure non tiene conto di altri requisiti di sicurezza specifici del settore, nonché di specifici obblighi normativi, derivanti ad esempio dalla direttiva e-privacy o dalla direttiva NIS. In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013 security controls is also included. Nel tentativo di facilitare ulteriormente questa procedura è inclusa anche una mappatura del gruppo di misure proposto con i controlli di sicurezza ISO / IEC 27001: 2013 .

Security policy and procedures for the protection of personal data Politica di sicurezza e procedure per la protezione dei dati personali

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
A.1 A.1	The organization should document its policy with regards to personal data processing as part of its information security policy. L'organizzazione dovrebbe documentare la propria politica in materia di trattamento dei dati personali nell'ambito della propria politica di sicurezza delle informazioni.	
A.2 A.2	The security policy should be reviewed and revised, if necessary, on an annual basis. La politica di sicurezza dovrebbe essere rivista e rivista, se necessario, su base annuale.	
	Related to ISO 27001:2013 - A.5 Security policy Relativo a ISO 27001: 2013 - A.5 Politica di sicurezza	

Roles and responsibilities Ruoli e responsabilità

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
B.1 B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy. I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.	
B.2 B.2	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined. Durante le riorganizzazioni interne o le cessazioni e il cambio di lavoro, la revoca dei diritti e delle responsabilità con le rispettive procedure di consegna dovrebbe essere chiaramente definita.	
	Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities Relativo a ISO 27001: 2013 - A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni	

Access control policy Politica di controllo dell'accesso

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
C.1 C.1	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle. Diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento dei dati personali) in seguito alla necessità di conoscere il principio.	
	Related to ISO 27001:2013 - A.9.1.1 Access control policy Relativo a ISO 27001: 2013 - A.9.1.1 Politica di controllo dell'accesso	

Resource/asset management Gestione risorse / risorse

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
D.1 D.1	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). L'organizzazione dovrebbe disporre di un registro delle risorse IT utilizzate per l'elaborazione dei dati personali (hardware, software e rete). The register could include at least the following information: IT resource, type (eg server, workstation), location (physical or electronic). Il registro potrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). A specific person should be assigned the task of maintaining and updating the register (eg IT officer). A una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad es. Responsabile IT).	
D.2 D.2	IT resources should be reviewed and updated on regular basis. Le risorse IT dovrebbero essere riviste e aggiornate su base regolare.	
	Related to ISO 27001:2013 - A.8 Asset management Relativo a ISO 27001: 2013 - A.8 Gestione delle risorse	

Change management Cambio gestione

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
E.1 E.1	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (eg IT or security officer). L'organizzazione dovrebbe assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad es. IT o responsabile della sicurezza). Regular monitoring of this process should take place. Dovrebbe essere effettuato un monitoraggio regolare di questo processo.	
E.2 E.2	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. Lo sviluppo del software deve essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. When testing is needed, dummy data should be used (not real data). Quando è necessario eseguire il test, è necessario utilizzare dati fittizi (non dati reali). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing. Nei casi in cui ciò non sia possibile, devono essere predisposte procedure specifiche per la protezione dei dati personali utilizzati durante i test.	
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities Relativo a ISO 27001: 2013 - A. 12.1 Procedure operative e responsabilità	

Data processors Responsabili del trattamento dei dati

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
F.1 F.1	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento (appaltatori / outsourcing) devono essere definite, documentate e concordate tra il responsabile del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy. Tali linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali previsto dalla politica di sicurezza dell'organizzazione.	
F.2 F.2	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay. Dopo aver scoperto una violazione dei dati personali, il responsabile del trattamento informa il responsabile del trattamento senza indebito ritardo.	
F.3 F.3	Formal requirements and obligations should be formally agreed between the data controller and the data processor. Requisiti e obblighi formali dovrebbero essere concordati formalmente tra il responsabile del trattamento e il responsabile del trattamento. The data processor should provide sufficient documented evidence of compliance. Il responsabile del trattamento dei dati dovrebbe fornire prove documentate sufficienti della conformità.	
	Related to ISO 27001:2013 - A.15 Supplier relationships Relativo a ISO 27001: 2013 - A.15 Rapporti con i fornitori	

Incidents handling / Personal data breaches Gestione degli incidenti / Violazione dei dati personali

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
G.1 G.1	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data. È necessario definire un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.	
G.2 G.2	Personal data breaches should be reported immediately to the management. Le violazioni dei dati personali devono essere segnalate immediatamente alla direzione. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. Dovrebbero essere predisposte procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 and 34 GDPR. 33 e 34 GDPR.	
	Related to ISO 27001:2013 - A.16 Information security incident management Relativo a ISO 27001: 2013 - A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni	

Business continuity Business continuity

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
H.1 H.1	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach). L'organizzazione dovrebbe stabilire le principali procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema IT che elabora i dati personali (in caso di incidente / violazione dei dati personali).	

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
	Related to ISO 27001:2013 - A. 17 Information security aspects of business continuity management Relativo a ISO 27001: 2013 - A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa	

Confidentiality of personnel Riservatezza del personale

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
I.1 I.1	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. L'organizzazione dovrebbe garantire che tutti i dipendenti comprendano le proprie responsabilità e obblighi relativi al trattamento dei dati personali. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process. I ruoli e le responsabilità dovrebbero essere chiaramente comunicati durante il processo di pre-assunzione e / o di inserimento.	
	Related to ISO 27001:2013 - A.7 Human resource security Relativo a ISO 27001: 2013 - A.7 Sicurezza delle risorse umane	

Training Formazione

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
J.1 J.1	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. L'organizzazione dovrebbe garantire che tutti i dipendenti siano adeguatamente informati sui controlli di sicurezza del sistema IT relativi al loro lavoro quotidiano. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati sui requisiti pertinenti in materia di protezione dei dati e sugli obblighi legali attraverso regolari campagne di sensibilizzazione.	
	Related to ISO 27001:2013 - A.7.2.2 Information security awareness, education and training Relativo a ISO 27001: 2013 - A.7.2.2 Consapevolezza, istruzione e formazione della sicurezza delle informazioni	

Access control and authentication Controllo accessi e autenticazione

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
K.1 K.1	An access control system applicable to all users accessing the IT system should be implemented. È necessario implementare un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. The system should allow creating, approving, reviewing and deleting user accounts. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	
K.2 K.2	The use of common user accounts should be avoided. L'uso di account utente comuni dovrebbe essere evitato. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities. Nei casi in cui ciò è necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
K.3 K.3	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). Dovrebbe essere istituito un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). As a minimum a username/password combination should be used. È necessario almeno una combinazione nome utente / password. Passwords should respect a certain (configurable) level of complexity. Le password devono rispettare un certo livello (configurabile) di complessità.	
K.4 K.4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity. Il sistema di controllo degli accessi dovrebbe avere la capacità di rilevare e non consentire l'uso di password che non rispettano un certo livello (configurabile) di complessità.	
	Related to ISO 27001:2013 - A.9 Access control Relativo a ISO 27001: 2013 - A.9 Controllo degli accessi	

Logging and monitoring Registrazione e monitoraggio

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
L.1 L.1	Log files should be activated for each system/application used for the processing of personal data. I file di registro devono essere attivati per ciascun sistema / applicazione utilizzata per il trattamento dei dati personali. They should include all types of access to data (view, modification, deletion). Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	
L.2 L.2	Log files should be timestamped and adequately protected against tampering and unauthorized access. I file di registro devono essere timestamp e adeguatamente protetti da manomissioni e accessi non autorizzati. Clocks should be synchronised to a single reference time source Gli orologi dovrebbero essere sincronizzati con una singola sorgente temporale di riferimento	
	Related to ISO 27001:2013 - A.12.4 Logging and monitoring Relativo a ISO 27001: 2013 - A.12.4 Registrazione e monitoraggio	

Server/Database security Sicurezza server / database

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
M.1 M.1	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly. I server di database e applicazioni devono essere configurati per essere eseguiti utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	
M.2 M.2	Database and applications servers should only process the personal data that are actually needeeds to process in order to achieve its processing purposes. I database e i server delle applicazioni devono elaborare solo i dati personali che sono effettivamente necessari al fine di raggiungere i suoi scopi di elaborazione.	
	Related to ISO 27001:2013 - A. 12 Operations security Relativo a ISO 27001: 2013 - A. 12 Sicurezza operativa	

Workstation security Sicurezza della workstation

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
N.1 N.1	Users should not be able to deactivate or bypass security settings. Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	
N.2 N.2	Anti-virus applications and detection signatures should be configured on a weekly basis. Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base settimanale.	
N.3 N.3	Users should not have privileges to install or deactivate unauthorized software applications. Gli utenti non dovrebbero avere privilegi per installare o disattivare applicazioni software non autorizzate.	
N.4 N.4	The system should have session time-outs when the user has not been active for a certain time period. Il sistema dovrebbe avere dei timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	
N.5 N.5	Critical security updates released by the operating system developer should be installed regularly. Gli aggiornamenti critici per la sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems Relativo a ISO 27001: 2013 - A. 14.1 Requisiti di sicurezza dei sistemi di informazione	

Network/Communication security Sicurezza di rete / comunicazione

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
O.1 O.1	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL). Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	
	Related to ISO 27001:2013 - A.13 Communications Security Relativo a ISO 27001: 2013 - A.13 Sicurezza delle comunicazioni	

Back-ups Back-up

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
P.1 P.1	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities. Le procedure di backup e ripristino dei dati dovrebbero essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	
P.2 P.2	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data. Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati ai dati di origine.	
P.3 P.3	Execution of backups should be monitored to ensure completeness. L'esecuzione dei backup deve essere monitorata per garantire la completezza.	
P.4 P.4	Full backups should be carried out regularly. I backup completi devono essere eseguiti regolarmente.	
	Related to ISO 27001:2013 - A.12.3 Back-Up Relativo a ISO 27001: 2013 - A.12.3 Backup	

Mobile/Portable devices Dispositivi mobili / portatili

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
Q.1 Q.1	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use. Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	
Q.2 Q.2	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized. I dispositivi mobili autorizzati ad accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	
Q.3 Q.3	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment. I dispositivi mobili dovrebbero essere soggetti agli stessi livelli di procedure di controllo dell'accesso (al sistema di elaborazione dati) delle altre apparecchiature terminali.	
	Related to ISO 27001:2013 - A. 6.2 Mobile devices and teleworking Relativo a ISO 27001: 2013 - A. 6.2 Dispositivi mobili e telelavoro	

Application lifecycle security Sicurezza del ciclo di vita delle applicazioni

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
R.1 R.1	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed. Durante il ciclo di vita dello sviluppo dovrebbero essere seguite le migliori pratiche, quadri e standard di sviluppo sicuri ben noti e all'avanguardia.	
R.2 R.2	Specific security requirements should be defined during the early stages of the development lifecycle. Requisiti specifici di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	
R.3 R.3	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements. Tecnologie e tecniche specifiche progettate per supportare la privacy e la protezione dei dati (anche denominate Tecnologie per il miglioramento della privacy (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
R.4 R.4	Secure coding standards and practises should be followed. Devono essere seguiti standard e pratiche di codifica sicuri.	
R.5 R.5	During the development, testing and validation against the implementation of the initial security requirements should be performed. Durante lo sviluppo, dovrebbero essere eseguiti test e validazione contro l'implementazione dei requisiti di sicurezza iniziali.	
	Related to ISO 27001:2013 - A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes Relativo a ISO 27001: 2013 - A.12.6 Gestione delle vulnerabilità tecniche e A.14.2 Sicurezza nei processi di sviluppo e supporto	

Data deletion/disposal Cancellazione / smaltimento dei dati

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
S.1 S.1	Software-based overwriting should be performed on all media prior to their disposal. La sovrascrittura basata su software deve essere eseguita su tutti i supporti prima della loro eliminazione. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed. Nei casi in cui ciò non sia possibile (CD, DVD, ecc.) Dovrebbe essere eseguita la distruzione fisica.	
S.2 S.2	Shredding of paper and portable media used to store personal data shall be carried out. Deve essere eseguita la triturazione della carta e dei supporti portatili utilizzati per archiviare i dati personali.	
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment Relativo a ISO 27001: 2013 - A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento sicuro o riutilizzo delle apparecchiature	

Physical security Sicurezza fisica

Measure Identifier Identificatore di misura	Measure Description Descrizione della misura	Risk level Livello di rischio
T.1 T.1	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel. Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile a personale non autorizzato.	
	Related to ISO 27001:2013 - A.11 – Physical and environmental security Relativo a ISO 27001: 2013 - A.11 - Sicurezza fisica e ambientale	