



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

I.S.I.S.S. "G.VERDI"-VALDOBBIADENE
Prot. 0006162 del 10/08/2021
A 32 (Uscita)

ISISS "G. Verdi"

Titolo documento: Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

Codice documento: DOC021

Stato documento: Definitivo

Versione: 7.0

Data creazione: 2 settembre 2018

Data ultimo aggiornamento 1 agosto 2019



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

1. Obiettivo della Procedura Operativa

Obiettivo della presente procedura operativa è fornire al soggetto designato “custode delle password di sistema” una guida operativa per la custodia in sicurezza delle password relative al profilo di administrator degli apparati, dei sistemi e dei programmi utilizzati dall’Ente.

Infatti una non corretta gestione delle password può compromettere in maniera grave e significativa la sicurezza dei dati e/o dei programmi; ad esempio nel caso le password non siano custodite in un luogo sicuro (es. cassaforte o armadio blindato) ciò può compromettere la riservatezza dei dati; nel caso invece non siano custodite tutte le password, ciò può compromettere la disponibilità dei dati, nel caso sia necessario accedere ai dati in situazione di emergenza.

2. Criticità principali che la Procedura Operativa indirizza

Nel processo di gestione delle password si verificano tipicamente alcune situazioni di criticità/rischio, che sono opportunamente gestite dalla presente procedura operativa. Di seguito

si riportano le principali criticità e gli approcci messi in atto per contrastarle.

CRITICITA’ N. 1: ASSENZA DI ALCUNE PASSWORD

Una delle più frequenti criticità che si verificano nel processo di gestione delle password è l’assenza o indisponibilità di alcune password: vale a dire che il custode delle password di sistema non ha a disposizione tutte le password di sistema. Questo si verifica spesso perché non viene redatto e tenuto regolarmente aggiornato un inventario degli apparati e dei sistemi ai quali è necessario accedere con profilo di administrator.



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

Il custode delle password non ha quindi a disposizione un inventario, un elenco per verificare se le password in suo possesso sono tutte quelle definite, oppure se ve ne siano di mancanti.

**STRATEGIA MESSA IN ATTO PER CONTRASTARE LA CRITICITA' N. 1
(ASSENZA DI ALCUNE PASSWORD)**

Per contrastare la criticità consistente nell'assenza di alcune password, si dovrà predisporre e tenere regolarmente aggiornato un inventario dei sistemi, articolato in sistemi hardware (es. server, router, firewall etc.), sistemi software di base (es. sistemi operativi, DBMS – Sistemi per la gestione di basi di dati, sistemi per la gestione di posta elettronica etc.) e software applicativi. In questo modo sarà possibile fare periodicamente una sorta di “appello” per verificare che siano custodite e disponibili in caso di necessità tutte le password necessarie.

CRITICITA' N. 2: PASSWORD NON AGGIORNATE

Un'altra tra le criticità che si verificano frequentemente è rappresentata dal fatto che le password custodite non sono aggiornate, e sono di fatto “vecchie”; questo si verifica allorché l'amministratore di sistema (sia esso un soggetto interno o esterno) modifica la password e non la comunica (o meglio non la consegna in busta chiusa) al custode delle password.

**STRATEGIA MESSA IN ATTO PER CONTRASTARE LA CRITICITA' N. 2
(PASSWORD NON AGGIORNATE)**

Una prima strategia consiste nel tenere un registro dei cambi di password, e piuttosto che “subire” il processo, diventarne attori: vale a dire che periodicamente, ad esempio ogni sei mesi, il custode delle password chiederà all'amministratore di



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

sistema di modificare la password, e pretenderà di ottenere in busta chiusa la nuova password.

Una seconda strategia consiste nel fare dei controlli a campione, volti a verificare che le password custodite siano effettivamente quelle definite in quel momento.

CRITICITA' N. 3: PASSWORD RIPORTATE NEL MEDESIMO FOGLIO

Una terza criticità piuttosto frequente consiste nel fatto che le password sono riportate su un unico foglio; in questo caso, se è necessario accedere ad esempio alla password relativa all'apparato firewall, essendo le password riportate nel medesimo foglio, chi ha accesso al foglio prenderà conoscenza non solo della password necessaria (relativa al firewall), ma a tutte le altre password, compromettendo in questo modo la riservatezza di tutte le password.

STRATEGIA MESSA IN ATTO PER CONTRASTARE LA CRITICITA' N. 3 (PASSWORD RIPORTATE NEL MEDESIMO FOGLIO)

Per contrastare la criticità si dovrà avere cura di riportare una sola password su ciascun foglio custodito all'interno di una busta chiusa e sigillata. Questo significa ad esempio che se in tutto sono definite dieci password, non si dovrà avere un foglio con l'elenco delle dieci password, ma si dovranno avere dieci buste chiuse, ciascuna contenente una sola password.



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

**ATTORE PRINCIPALE DELLA PROCEDURA OPERATIVA : CUSTODE
DELLE PASSWORD DI SISTEMA**

**ATTORI SECONDARI COINVOLTI: AMMINISTRATORE DI SISTEMA
INTERNO, AMMINISTRATORE DI SISTEMA ESTERNO, FIDUCIARIO**

PASSI OPERATIVI

N.	Input	Descrizione	Output	Note
1	Inventario risorse hardware e software	Dall'inventario delle risorse hardware e software ricavare un elenco degli account di administrator e determinare il numero N_A di account	Inventario degli account di administrator	
2	Inventario degli account di administrator	Verificare che il numero di buste chiuse custodite sia maggiore o uguale al numero N_A . Nel caso vi siano meno buste, richiedere all'amministratore di sistema le password mancanti	Richiesta password mancanti	A seconda dei casi, la richiesta dovrà essere rivolta ad un soggetto interno oppure esterno
3	Registro cambi password	Nel caso dalla consultazione del registro risultino esistere password non modificate da più di sei mesi,	Richiesta password mancanti	A seconda dei casi, la richiesta dovrà essere rivolta ad un soggetto interno oppure esterno



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

		richiedere all'amministratore di sistema di modificare le password modificate e comunicarle in busta chiusa		
4	Password mancanti	Una volta ricevute le password mancanti, si dovrà verificare che la busta sia chiusa, firmata e datata sul lato esterno, protocollata e riportante l'identificativo del sistema e dell'account al quale la password si riferisce. Si dovrà inoltre aggiornare il registro dei cambi password	Registro cambi password aggiornato.	
5	Richiesta password	All'atto di una richiesta di password, si dovranno attentamente verificare le seguenti circostanze: <ul style="list-style-type: none">• che la richiesta sia lecita e improrogabile	Tentativi di contattare l'amministratore di sistema	



Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

		<ul style="list-style-type: none">• che il sistema sia “di competenza” del soggetto richiedente• che l’amministratore di sistema sia effettivamente assente o indisponibile		
6	Buste chiuse custodite in cassaforte	Solo nel caso in cui le verifiche di cui al punto precedente siano state tutte esperite, e solo in caso di assenza o indisponibilità dell’amministratore di sistema, si potrà procedere all’apertura della cassaforte e al prelievo della busta contenente la password necessaria	Busta prelevata dalla cassaforte	
7	Busta prelevata dalla cassaforte	Alla presenza del fiduciario designato dall’amministratore di sistema, il custode delle password procederà all’apertura della busta contenente la password richiesta	Busta prelevata dalla cassaforte ed aperta in presenza del fiduciario designato dall’amministratore di sistema	



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

8	Busta prelevata dalla cassaforte ed aperta in presenza del fiduciario designato dall'amministratore di sistema	Alla presenza del fiduciario, ma senza che quest'ultimo prenda cognizione della password, il custode delle password digita la password e accede al sistema	Sistema reso disponibile mediante digitazione della password	
9		Il sistema viene ora messo a disposizione del soggetto richiedente. Il fiduciario e il custode delle password vigilano sull'operato del richiedente, verificando che siano compiute le operazioni strettamente indispensabili e non siano perpetrati abusi.	Operazioni effettuate sul sistema, sotto la vigilanza del fiduciario e del custode	
10		Una volta terminate le operazioni, alla presenza del fiduciario e del richiedente, il custode delle password redige sintetico verbale delle operazioni effettuate, firmato	Verbale delle operazioni effettuate	Il verbale deve essere comunicato o portato a conoscenza dell'amministratore di sistema alla prima occasione utile



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

		da tutti i soggetti (richiedente, fiduciario e custode delle password)		
11	Verbale operazioni effettuate	L'amministratore di sistema verifica che le operazioni effettuate corrispondano effettivamente a quelle dichiarate a livello di verbale	Verifica operazioni effettuate	
12	Modifica password	Poiché la password ha perso la segretezza, l'amministratore di sistema modifica la password	Password modificata	
13	Comunicazione password in busta chiusa	L'amministratore di sistema annota la nuova password e la colloca in busta chiusa, datata e firmata sul lato esterno e protocollata, e la consegna a mano al custode delle password	Nuova password comunicata in busta chiusa al custode delle password	



**I.S.I.S.S. G. VERDI
VALDOBBIADENE**

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Procedura Operativa per la custodia delle password di Sistema, ai sensi degli artt. 29 e 32 del GDPR

14		Il custode delle password riceve la nuova busta, la protocolla e aggiorna di conseguenza il registro dei cambi password	Registro cambi password aggiornato	
-----------	--	---	------------------------------------	--

La Dirigente scolastica
Giuliana Barazzuol