Spis treści:

Lp.	Data	Punkty zmienione	Krótki opis zmiany	Podpis

	Data	Imię i nazwisko	Podpis
Opracował	**2018-03-01**	**Daniel Opara**	
Zatwierdził	**2018-03-01**	**Michał Borkowski**	
Wydał	**2018-03-01**	**Michał Borkowski**	

1. Cel i przedmiot procedury

Celem procedury jest opisanie systemu i zasad postępowania podczas przetwarzania, przekazywania wyników oraz wykonywania i przechowywania kopii zapasowych zapisów w formie elektronicznej.

Przedmiotem procedury jest tryb postępowania z zapisami cyfrowymi rozumianymi jako: zlecenia, maile z istotnymi ustaleniami, rysunki i dokumentacją od klienta, wyniki w formie zestawień tabelarycznych, wyniki w formie sprawozdań. Procedura określa dostęp do danych, sposoby zabezpieczenia przed niepowołanym dostępem, przekazywanie wyników w formie elektronicznej oraz wykonywanie i przywracanie kopii zapasowych danych przechowywanych na serwerze plików oraz komputerach pracowników firmy.

2. Zakres stosowania

Procedura obowiązuje wszystkich pracowników korzystających w swojej pracy ze sprzętu komputerowego udostępnionego przez firmę.

3. Definicje

- Zlecenie – mail, zeskanowany fax lub elektroniczny zapis z rozmowy telefonicznej od klienta zawierający zamówienie
- Istotne ustalenia – informacja zmieniająca/uzupełniająca wymagania lub zakres usług świadczonych przez Navitest
- Zestawienia tabelaryczne – zbiorcze wyniki badań na serwerze wewnętrznym lub przestrzeni typu chmura Google
- Zewnętrzny serwer FTP – serwer udostępniający usługę FTP znajdujący się poza strukturą teleinformatyczną firmy Navitest
- Komputer użytkownika – komputer należący do firmy Navitest, będący w użytkowaniu przez pracownika firmy Navitest
- Serwer plików – serwer znajdujący się w wewnętrznej sieci teleinformatycznej firmy Navitest umożliwiający pracownikom przechowywanie i współdzielenie plików z innymi użytkownikami sieci wewnętrznej
- Sieć wewnętrzna – wewnętrzna sieć teleinformatyczna firmy Navitest
- Lokalna kopia zapasowa – kopia wykonana przez program typu backup i zapisana bezpośrednio na nośniku danych zamontowanym na stałe w komputerze użytkownika
- Repozytorium - miejsce uporządkowanego przechowywania dokumentów na serwerze, których wszystkie zapisy przeznaczone są do udostępniania. Magazyn główny, zaprojektowany w taki sposób, aby dostęp do wszystkich jego zasobów był równie łatwy. Przechowywane są w nim archiwalne kopie i wersje dokumentów.

4. Odpowiedzialność

4.1. Odpowiedzialność za treść niniejszej procedury ponosi Kierownik Techniczny Laboratorium. Odpowiedzialność za oprogramowanie, ustawienia i działanie serwerów, repozytoriów, systemu wykonywania kopii zapasowych ponosi informatyk zatrudniony przez firmę Navitest.
4.2. Za wdrożenie i nadzór nad przestrzeganiem niniejszej procedury odpowiada Kierownik Techniczny Laboratorium.
4.3. Odpowiedzialność za stosowanie zasad niniejszej procedury podczas użytkowania powierzonego sprzętu ponosi pracownik.

5. Opis sposobu postępowania

5.1 Dostęp do danych

5.1.1 Dla pracowników
Wszystkie komputery stacjonarne i przenośne są zabezpieczone loginem i hasłem zmienianym nie rzadziej niż raz na sześć miesięcy. Pracownik pozostawiając komputer bez nadzoru zobowiązany jest do przejścia na ekran logowania (np. używając klawiszy WIN+L). Serwery poczty, plików roboczych, zeskanowanych sprawozdań są zabezpieczone loginem i hasłem.

5.1.2 Dla klientów
Udostępnianie elektronicznych wersji sprawozdań na zewnętrznym serwerze FTP wymaga użycia loginu i hasła.

5.2 Bezpieczeństwo dokumentów elektronicznych.

5.2.1 Bezpieczeństwo zapewnia się poprzez:
- właściwe zasilanie sprzętu stosując wydzielone linie zasilania energetycznego dla komputerów i serwerów pracujących w sieci oraz systemy zasilania awaryjnego UPS,
- tworzenie kopii zapasowych zgodnie z instrukcją ***NVT/IN/O-3.2***,
- stosowanie programów antywirusowych na wszystkich stanowiskach komputerowych,
- zabezpieczenie sieci komputerowej przed dostępem z zewnątrz,
- brak bezpośredniego dostępu do serwera z sieci publicznej
- administracja serwerem odbywa się tylko przez szyfrowaną usługę SSH
- usługa SSH została skonfigurowana tak, aby nie działała na standardowym porcie dla tej usługi
- do usługi SSH można się zalogować tylko na konto użytkownika. Bezpośrednie zalogowanie na konto administratora serwera jest niemożliwe.
- dostęp do serwera od strony sieci publicznej jest ograniczony przez firewall ustawiony na ruterze dostępowym.

5.2.2 Zabezpieczenia serwera pocztowego:
- wysyłanie i odbieranie poczty odbywa się dopiero po autoryzacji użytkownika (podanie loginu i hasła)
- wysyłanie danych poczty jest szyfrowane przy użyciu protokołu SSL
- odbiór poczty może się odbywać przy użyciu szyfrowania SSL.

5.2.3 Zabezpieczenia zewnętrznego serwera FTP (dla klienta):
- autoryzacja użytkownika przez podanie loginu i hasła,
- połączenie szyfrowane za pomocą SSL,
- serwer FTP jest używany tylko do uploadu danych.

Komunikacja serwer - kontrahent odbywa się po autoryzacji kontrahenta loginem oraz hasłem.

5.3 Nadzorowanie sprzętu komputerowego.

Kierownik techniczny prowadzi rejestr sprzętu komputerowego użytkowanego w Firmie poprzez system OCS Inventory oraz listę elektroniczną w repozytorium ISO. Lista zawiera ***„Rejestr awarii sprzętu komputerowego”,*** w którym odnotowuje wszystkie zgłoszone przez pracowników awarie sprzętu i dokonane przeglądy lub naprawy.

Kierownik techniczny do przeglądu sprzętu komputerowego wyznacza serwisanta, który jest odpowiedzialny za okresowe sprawdzanie użytkowanego sprzętu.
Szczegółowy opis nadzorowania sprzętu komputerowego znajduje się w instrukcji ***NVT/IN/O-3.1***.

5.4. Miejsca gromadzenia danych elektronicznych

W Laboratorium do zapisu danych elektronicznych oraz zeskanowanych oryginalnych sprawozdań z badań używamy poniższych lokalizacji:
- dla wersji .doc oraz zeskanowanych sprawozdań, dokumentacji od klienta - wewnętrzny serwer plików,
- dla sprawozdań w pdf udostępnianych klientowi – zewnętrzny serwer FTP,
- dokumentacja systemu jakości, procedury oraz normy – repozytoria, fizycznie umieszczone na serwerze plików,
- listy sprawozdań, listy badań planowych – dysk Google,
- poczta elektroniczna – zewnętrzny serwer,
- dokumentacja firmowa członków kierownictwa – komputer użytkownika,
- kopie zapasowe dokumentów kierownictwa – serwer plików,
- kopie zapasowe serwera plików – zewnętrzny serwer FTP.

5.5. Sposoby przekazywania wyników badań w formie elektronicznej

Preferowaną formą przekazywania wyników jest udostępnianie:
- sprawozdań poprzez serwer FTP,
- roboczych zestawień wyników w formie np. list badań planowych przez dysk Google (z wyłączeniem możliwości edycji).

Dopuszczalną formą przekazywania wyników jest email.

6. Kopie zapasowe

W Laboratorium kopie zapasowe należy wykonywać zgodnie z instrukcją ***NVT/IN/O-3.2.***

7. Repozytoria

7.1 Dostęp do repozytorium mają tylko wybrani użytkownicy. Każdy użytkownik przed uzyskaniem dostępu do danych przechowywanych w repozytorium musi zostać zautoryzowany poprzez podanie nazwy użytkownika oraz hasła. Rodzaj dostępu: pełny lub tylko do odczytu nadaje Kierownik Techniczny.
7.2 Repozytorium po stronie serwera jest realizowane przez program SVN. Po stronie klienta, czyli na komputerach pracowników usługa dostępu do serwera repozytorium jest realizowana przez oprogramowanie „Tortoise SVN".
7.3 Przywracanie kopii zapasowej
Za pomocą programu **„Tortoise SVN"** należy pobrać odpowiednią wersje pliku lub folderu z repozytorium.

8. Załączniki

- ***NVT/IN/O-3.1 Instrukcja nadzorowania sprzętu komputerowego***
- ***NVT/IN/O-3.2 Instrukcja tworzenia kopii zapasowych***