

	PROCEDURA			XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris			
	BUS	TRAM	Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego				Strona 1 z 9

I. Cel

Celem niniejszego dokumentu jest określenie zasad właściwego użytkowania systemów i sprzętu teleinformatycznego stanowiącego własność spółki Solaris Bus & Coach S.A.

II. Zakres stosowania

Niniejszy dokument przedstawia politykę Solaris w zakresie:

- właściwego korzystania przez użytkowników z danych i systemów teleinformatycznych będących w posiadaniu Solaris,
- dostępu użytkowników do Internetu dostarczonego przez Solaris,
- wiadomości wysyłanych i otrzymywanych przez użytkowników m.in. w ramach systemu poczty elektronicznej Solaris.

Zapisy niniejszego dokumentu obowiązują wszystkie osoby lub podmioty, które korzystają z systemów teleinformatycznych Solaris lub mają do nich dostęp, bez względu na rodzaj umowy zawartej z Solaris.

III. Dokumenty bazowe, pojęcia

- Norma ISO 9001
- Norma ISO 14001
- Norma ISO 3834-2
- Księga Zintegrowanego Systemu Zarządzania
- IRIS

Powyższe dokumenty są dostępne w zasobach spółki.

Pojęcia:

Solaris - Solaris Bus & Coach S.A.

Własność Solaris - Solaris jest właścicielem systemu bądź sprzętu teleinformatycznego lub Solaris jest uprawniony do korzystania z systemu/sprzętu na podstawie innego tytułu prawnego.

System teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania (licencje, oprogramowanie i systemy, etc.) oraz wszelkich innych zespołów zapewniających przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych teleinformatycznych poprzez sieci telekomunikacyjne, które stanowią własność Solaris lub do których użytkowania Solaris przysługuje prawo.

Sprzęt teleinformatyczny - fizyczne urządzenia informatyczne stanowiące część systemu teleinformatycznego w tym m.in. notebook, PC, telefon stacjonarny, telefon komórkowy, drukarka, skaner, myszka, klawiatura, monitor, pendrive, tablet, dysk pamięci, karty pamięci etc., do których użytkowania Solaris przysługuje prawo.

Kierownik Obszaru IT - osoba mianowana i upoważniona przez Dyrektora Działu IT, odpowiedzialna za wdrożenie, nadzór i stosowanie dokumentów Systemu Bezpieczeństwa Informacji oraz wszystkich zarządzeń wewnętrznych w obszarze, za który pełni odpowiedzialność.

Administrator/Programista/Konsultant/Specjalista - osoba/y wymienione imiennie posiadające upoważnienie nadane przez Kierownika Obszaru IT lub Dyrektora IT do nadzorowania pracy systemu teleinformatycznego.

Helpdesk - zespół odpowiedzialny za przyjmowanie zgłoszeń od użytkowników oraz kontrolę ich rozwiązania.

Użytkownik - osoba fizyczna korzystająca z systemów teleinformatycznych.

Pracownik - osoba fizyczna, posiadająca umowę o pracę z Solaris.

Autor dokumentu (sporządził)		Właściciel procesu lub Dyrektor Działu (sprawdził)	
Data	Podpis	Data	Podpis
Pełnomocnik Zarządu ds. ZSZ (kontroluje)		Zarząd (zatwierdził)	
Data	Podpis	Data	Podpis

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	<u>BUS</u>	<u>TRAM</u>		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 2 z 9

Dane teleinformatyczne - wszelkie informacje posiadane, przetwarzane, przechowywane lub przesyłane za pomocą systemów teleinformatycznych Solaris.

Dane osobowe - oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Kontrahent - podmiot, organizacja, lub osoba fizyczna, posiadająca umowę o współpracy, umowę o dzieło, o konsultacje lub z którym Solaris współpracuje w inny sposób.

Informacje poufne - wszelkie informacje, materiały, dokumenty, dane w formie ustnej, pisemnej, elektronicznej lub utrwalane w inny sposób, w których posiadaniu znajduje się Solaris, w tym w szczególności dane finansowe i prawne, dane dotyczące strategii sprzedaży, reklamy, promocji, wszelkie dane techniczne i technologiczne dotyczące produkcji, jak również technologii, ich naprawy i serwisowania produktów (know - how), a także dotyczące rzeczywistych i potencjalnych klientów i kontrahentów Solaris, udostępniane bezpośrednio lub za pośrednictwem osób działających w imieniu Solaris, lub które zostaną uzyskane przy okazji wykonywania umowy zawartej z Solaris, a także wszelkie informacje określone jako „poufne”.

Normalny tok pracy - wszelkie czynności wykonywane w celu świadczenia pracy lub usług na rzecz i w ramach umowy zawartej z Solaris.

System Bezpieczeństwa Informacji - jest zbiorem reguł i procedur, według których są budowane, zarządzane oraz udostępniane systemy informatyczne. Określa ona, które elementy i w jaki sposób mają być chronione.

Intranet - wewnętrzny portal informacyjny Solaris oparty na technologii przeglądarkowej (www).

Materiały niedozwolone - dane (bez względu na formę ich zapisu), które zawierają treści o charakterze obraźliwym, rasistowskim, seksistowskim, pornograficznym, szkalującym bądź napastliwym wobec osób lub podmiotów trzecich.

Wirus komputerowy - program komputerowy posiadający samodzielną zdolność powielania się, tak jak prawdziwy wirus. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz zachowanie użytkownika komputera. Może spowodować nieprawidłowe działanie systemu komputerowego.

Robak komputerowy - samoreplikujący się program komputerowy, który może spowodować nieprawidłowe działanie systemu komputerowego.

Koń trojański, trojan - oprogramowanie, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementuje niepożądane, ukryte przed użytkownikiem różne funkcje.

IV. Odpowiedzialności

4.1. Użytkownicy odpowiadają za:

4.1.1. Odpowiedzialność – systemy teleinformatyczne:

- bezpieczeństwo, poufność, spójność i przechowywanie zapisanych danych zgodnie z zasadami niniejszej procedury,
- skanowanie danych pochodzących z nośników zewnętrznych,
- informowanie Helpdesk o wykryciu wirusa,
- oznaczenie danych jako prywatne.

4.1.2. Odpowiedzialność – sprzęt teleinformatyczny:

- utrzymanie sprzętu teleinformatycznego w dobrym stanie technicznym i zapewnienie jego bezpieczeństwa,
- obowiązkowo zgłoszenie na Policję oraz niezwłoczne zgłoszenie przełożonemu i Działowi IT przypadków kradzieży,
- niezwłoczne zgłoszenie przełożonemu i Działowi IT uszkodzenia, zniszczenia, zagubienia sprzętu teleinformatycznego. Pełną odpowiedzialność finansową za powierzony sprzęt ponosi użytkownik,
- najpóźniej w dniu ustania stosunku pracy użytkownik zobowiązany jest do zwrotu powierzonego sprzętu. Bezpośredni przełożony użytkownika (zgodnie ze strukturą organizacyjną obowiązującą na ostatni dzień pracy użytkownika) zobowiązany jest do dopilnowania zrealizowania tego obowiązku. W przypadku nie wywiązania się z tego obowiązku przez użytkownika bezpośredni przełożony ponosić może z tego tytułu odpowiedzialność dyscyplinarną.

4.2. Dyrektor IT odpowiada za:

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	BUS	TRAM		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 3 z 9

- wdrożenie, nadzór i stosowanie dokumentów Systemu Bezpieczeństwa Informacji,
- nadzór nad przestrzeganiem wszystkich zarządzeń wewnętrznych w obszarze IT,
- ostateczne zatwierdzanie wyboru technologii, sprzętu i konfiguracji technicznej dla Solaris.

4.3. Kierownik Obszaru IT odpowiada za:

- wdrożenie, nadzór i stosowanie dokumentów Systemu Bezpieczeństwa Informacji w obszarze za który pełni odpowiedzialność,
- przestrzeganie wszystkich zarządzeń wewnętrznych w obszarze IT za który pełni odpowiedzialność.

4.4. Administrator/Programista/Konsultant/Specjalista Administrator odpowiada za:

- przyznawanie dostępu do systemu informatycznego na poziomie administracyjnym,
- nadawanie uprawnień administracyjnych użytkownikom zewnętrznym,
- odbieranie uprawnień administracyjnych,
- nadzorowania pracy systemu informatycznego służącego do przetwarzania danych,
- dodawania i kasowania kont użytkowników,
- przydzielania i usuwania dostępu,
- zapewnienia ciągłości pracy w systemie teleinformatycznym,
- nadzorowanie pracy serwerów,
- instalowanie oprogramowania,
- dbanie o bezpieczeństwo systemu teleinformatycznego,
- nadzorowania i eliminowania nieprawidłowości systemu teleinformatycznego.

4.5. Helpdesk odpowiada za:

- przyjmowanie zgłoszeń od użytkowników i administratorów,
- rozwiązywanie przyjmowanych zgłoszeń,
- przekierowywanie zgłoszeń do odpowiednich działów IT,
- kontrola rozwiązywania problemów.

V. Postępowanie w poszczególnych zakresach

5.1. Poufność informacji

- 5.1.1. Dane teleinformatyczne i systemy teleinformatyczne mają krytyczne znaczenie dla działalności Solaris, dlatego też konieczne jest wdrożenie i utrzymanie właściwego poziomu ochrony informacji w nich przechowanych. Niniejsza procedura przewiduje podjęcie działań mających na celu zabezpieczenie danych teleinformatycznych i systemów teleinformatycznych przed przypadkowym lub zamierzonym zniszczeniem, uszkodzeniem, modyfikacją lub wyjawieniem danych teleinformatycznych oraz utrzymanie odpowiedniego poziomu poufności, integralności, dostępności danych teleinformatycznych i systemów teleinformatycznych.
- 5.1.2. Użytkownicy powinni być świadomi ryzyka wynikającego z elektronicznego przechowywania informacji. Od użytkowników wymaga się podjęcia koniecznych środków ostrożności mających na celu ograniczenie związanych z tym zagrożeń.
Główne rodzaje ryzyka informacyjnego:
 - wyjawienie poufnych danych teleinformatycznych biznesowych lub informatycznych danych osobowych,
 - nieumyślne lub zamierzone usunięcie lub zmiana danych teleinformatycznych,
 - niedostępność danych teleinformatycznych.

5.2. Podstawowe zasady użytkowania systemów i sprzętu teleinformatycznego

- 5.2.1. Sprzęt teleinformatyczny, na którym działają systemy informatyczne dostarczone przez Solaris, wraz z tymi systemami, stanowi własność Solaris.
- 5.2.2. Wszelkie dane teleinformatyczne służbowe znajdujące się i stworzone na tym sprzęcie oraz w systemach teleinformatycznych Solaris również stanowią własność Solaris i nie powinny być usuwane, kopiowane lub udostępniane innym osobom bez wyraźnej zgody Solaris poza normalnym tokiem pracy.
- 5.2.3 Udostępnienie danych teleinformatycznych jest dopuszczalne, jeżeli jest to związane z normalnym tokiem wykonywanej pracy bądź wynika ze zlecenia przez Solaris określonych prac osobie trzeciej

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	<u>BUS</u>	<u>TRAM</u>		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 4 z 9

przy zgodzie przełożonego. Ponadto autorskie prawa majątkowe do wszelkich danych teleinformatycznych, w tym programów komputerowych, stworzonych przez pracowników lub użytkowników w wyniku wykonywania obowiązków wynikających ze stosunku pracy, przysługują wyłącznie Solaris. Dane teleinformatyczne nie mogą być usuwane, kopiowane i modyfikowane bez wyraźnej zgody Solaris.

- 5.2.4. Systemy teleinformatyczne Solaris oraz wszelkie dane teleinformatyczne w nich przechowywane są składnikami majątku o krytycznym znaczeniu dla działalności Solaris. Nadawanie wszelkich uprawnień do systemów teleinformatycznych odbywa się za pomocą złożenia wniosku dostępnego w zakładce szybki dostęp na Intranecie, które akceptowane są przez Kierownika IT i realizowane przez Administratora.
- 5.2.5. Użytkownicy zobowiązani są korzystać z systemów teleinformatycznych i urządzeń komputerowych i telekomunikacyjnych Solaris w sposób zgodny z prawem, zakresem obowiązków pracownika oraz z poszanowaniem innych użytkowników oraz kontrahentów. Z systemów komputerowych i urządzeń należy korzystać zgodnie z zapisami niniejszej procedury oraz stosownymi politykami, standardami i procedurami obowiązującymi w Solaris.
- 5.2.6. Niewłaściwe użytkowanie lub nadużywanie systemów teleinformatycznych i danych teleinformatycznych przez użytkownika może doprowadzić do podjęcia przez Solaris stosownych środków prawnych, w zależności od rodzaju nadużycia. Niewłaściwe użytkowanie lub nadużywanie systemów teleinformatycznych i danych teleinformatycznych przez użytkownika lub pracownika Solaris może skutkować konsekwencjami wynikającymi z obowiązującego prawa i/lub regulaminu pracy.
- 5.2.7. Użytkownicy powinni być świadomi, że kontaktując z innymi jednostkami przy użyciu systemów teleinformatycznych lub danych teleinformatycznych, mogą reprezentować oni w swych działaniach Solaris. Użytkownicy powinni być także świadomi, że ich działania mogą mieć wpływ na reputację Solaris oraz mogą powodować zaciągnięcie zobowiązań w imieniu Solaris i/lub użytkownika.
- 5.2.8. Użytkowanie systemów teleinformatycznych ma przede wszystkim pomagać w wykonywaniu obowiązków służbowych użytkownika dla i w imieniu Solaris. Przyzwolenie na ograniczony użytek prywatny, zgodnie z niniejszym dokumentem, pozostaje całkowicie w gestii Solaris. Użytkownik nie może oczekiwać lub twierdzić, że korzystanie z systemu teleinformatycznego w celach prywatnych jest jego prawem lub spodziewać się, że będzie ono traktowane jako kwestia prywatna.
- 5.2.9. Użytkownik wyraża zgodę na dostęp, przeglądanie oraz monitorowanie przez uprawniony personel sposobu użytkowania przez niego systemów teleinformatycznych, stosownie do rozdziału 5.8. niniejszej procedury, zgodnie z obowiązującym prawem.
- 5.2.10. W przypadku zagubienia lub kradzieży sprzętu teleinformatycznego będącego własnością Solaris należy natychmiast zgłaszać do Helpdesk, do przełożonego oraz na Policję, w celu podjęcia odpowiednich działań (zgłoszenie do ubezpieczyciela, zablokowania dostępu do firmowej sieci komputerowej).
- 5.2.11. Dostęp do systemów teleinformatycznych odbywa się poprzez system haseł:
 - hasła są indywidualne i przypisane wyłącznie dla pojedynczego użytkownika,
 - hasło muszą być co najmniej 8 znakowe,
 - nie wolno hasła drukować, zapisywać ani przechowywać w postaci elektronicznej,
 - hasło powinno być kombinacją liter, cyfr oraz znaków specjalnych,
 - hasło należy zmieniać co 60 dni,
 - nowe hasło musi być różne od 15 ostatnich haseł stosowanych przez użytkownika w danym systemie lub aplikacji,
 - brak dostępu do zasobu należy niezwłocznie zgłosić do Helpdesku.
- 5.2.12. Czas jaki dział IT potrzebuje na odtworzenie utraconej dokumentacji technicznej jest zależny od wielkości danych, które były zamieszczone na sieci oraz okresu z którego mają być one odzyskane. Czas ten jest określony w dokumencie dot. kopii zapasowych, który dostępny jest w dziale IT i może być przedstawiony upoważnionym do jego wglądu przez Kierownika Obszaru IT. Zasady tworzenia kopii bezpieczeństwa i archiwizowania danych teleinformatycznych zostały opisane w „Polityce kopii bezpieczeństwa i archiwizacji danych”, dostępnej w Dziale IT.

5.3. Użytkowanie systemów teleinformatycznych na terenie Solaris

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	<u>BUS</u>	<u>TRAM</u>		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 5 z 9

- 5.3.1. Zapotrzebowanie na nowy sprzęt teleinformatyczny należy zgłosić poprzez złożenie odpowiedniego wniosku dostępnego na stronie intranetowej.
- 5.3.2. Liczne aspekty komunikacji z wykorzystaniem systemu teleinformatycznego są chronione prawem własności intelektualnej. Pobranie, skopiowanie, posiadanie i dystrybuowanie materiałów pobranych z Internetu może stanowić naruszenie praw autorskich lub innych praw własności intelektualnej. Użytkownikom sieci lub systemów teleinformatycznych nie wolno pobierać ani rozpowszechniać pirackich programów lub danych teleinformatycznych pochodzących z nielegalnego źródła. Wszelkie pobrane programy lub pliki muszą być użytkowane zgodnie z odpowiednią licencją lub prawami autorskimi. W razie wątpliwości, przed pobraniem jakiegokolwiek materiału, użytkownicy powinni skontaktować się z Helpdeskiem.
- 5.3.3. Użytkownikom nie wolno umyślnie otwierać, pobierać lub rozpowszechniać materiałów niedozwolonych. Zabronione jest umyślne wyświetlanie jakiegokolwiek obrazu czy dokumentu stanowiącego materiał niedozwolony na sprzęcie komputerowym Solaris. Materiałów niedozwolonych nie wolno archiwizować, przechowywać, rozpowszechniać, edytować i zapisywać za pomocą systemów teleinformatycznych Solaris.
- 5.3.4. Użytkownikom nie wolno umyślnie starać się uzyskać dostępu do obszarów sieci, do których jest on ograniczony lub dokonywać prób dostępu do danych teleinformatycznych, które według ich wiedzy są poufne, lub o których powinni wiedzieć, że mają charakter poufny.
- 5.3.5. Użytkownikom nie wolno podejmować prób badania, skanowania lub łamania zabezpieczeń czy mechanizmów uwierzytliwiających systemów lub sieci zarówno wewnątrz, jak i na zewnątrz sieci Solaris.
- 5.3.6. Użytkownikom sieci lub systemów teleinformatycznych nie wolno świadomie rozpowszechniać wirusów, robaków, koni trojańskich i innych złośliwych programów komputerowych. Jeżeli użytkownik wykryje jakiegokolwiek wirusa, robaka, konia trojańskiego lub inny szkodliwy kod komputerowy, jest on zobowiązany do natychmiastowego przerwania pracy w systemie oraz bezzwłocznego zgłoszenia faktu wykrycia takiego programu do Helpdesku.
- 5.3.7. Użytkownicy są zobowiązani do powiadomienia Helpdesku, jeżeli odwiedzający ich gość zechce przyłączyć do
- przewodowej sieci Solaris komputer lub inne urządzenie nie będące własnością Solaris. Przyłączenie się do przewodowej sieci Solaris upoważnia Helpdesk do sprawdzenia sprzętu pod kątem zabezpieczeń antywirusowych i podatności na niebezpieczeństwa.
 - do sieci bezprzewodowej udzielany jest gościowi, dostawcy, konsultantowi czy kontrahentowi na wniosek osoby zapraszającej. W celu uzyskania dostępu należy zgłosić się do pracowników recepcji lub sekretariatu.
- 5.3.8. Użytkownikom nie wolno instalować nieautoryzowanego przez Helpdesk sprzętu lub oprogramowania. Każdy sprzęt i oprogramowanie musi być zatwierdzone przez Helpdesk.
- 5.3.9. Użytkownikom systemów teleinformatycznych nie wolno świadomie blokować lub przeciążać sieci komputerowej, jak również obchodzić mechanizmów służących ochronie prywatności lub bezpieczeństwa innego użytkownika.
- 5.3.10. Użytkownicy nie mogą zezwalać na używanie swojego konta i hasła przez nikogo innego, niezależnie od tego, czy osoba ta została upoważniona do dostępu do danych teleinformatycznych. Użytkownik ponosi odpowiedzialność za wszystkie operacje przeprowadzone z użyciem jego konta i hasła. Zgodę na dostęp do danych teleinformatycznych konta może wyrazić wyłącznie przełożony.
- 5.3.11. Użytkownikom sprzętu teleinformatycznego nie wolno używać narzędzi, oprogramowania lub kodów, które umożliwiają obejście mechanizmów bezpieczeństwa systemu komputerowego (włącznie z oprogramowaniem do podsłuchiwania pakietów).
- 5.3.12. Użytkownicy systemów teleinformatycznych są zobowiązani do stosownego zapisu i przechowywania danych teleinformatycznych zgodnie z regulacjami obowiązującymi w Solaris. Bezpiecznie przechowywane muszą być w szczególności wszystkie kopie poufnych informacji biznesowych na serwerach sieciowych udostępnianych tylko uprawnionym użytkownikom, lub przenoszone na zewnętrznych nośnikach jak płyta CD, pamięć przenośna lub wydruki. Krytyczne służbowe dane teleinformatyczne powinny być przechowywane na serwerach sieciowych.

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	<u>BUS</u>	<u>TRAM</u>		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 6 z 9

- 5.3.13. Użytkownicy są zobowiązani podejmować stosowne kroki zmierzające do fizycznego zabezpieczenia sprzętu, systemów i danych teleinformatycznych będących w ich posiadaniu. Użytkownicy są zobowiązani do bezpiecznego przechowywania urządzeń przenośnych oraz do blokowania stanowiska pracy, używając np. używając klawisza z logo systemu Windows i L, gdy pozostawia się je bez nadzoru. Wszelkie hasła użytkownik zobowiązany jest utrzymywać w tajemnicy i zabronione jest ich ujawnianie jakiejkolwiek innej osobie.
- 5.3.14. Użytkownicy systemów teleinformatycznych zobowiązani są zgłaszać wszelkie znane przypadki naruszenia postanowień niniejszej procedury do Helpdesku.
- 5.3.15. Nieprzestrzeganie powyższych zasad będzie stanowić naruszenie zapisów niniejszej procedury, jak również może stanowić m.in. następujące przestępstwa w świetle polskiego prawa:
- nieupoważniona modyfikacja materiałów komputerowych,
 - nieupoważniony dostęp do materiałów komputerowych (tzn. haking),
 - nieupoważniony dostęp w celu popełnienia przestępstwa lub umożliwienia kolejnych przestępstw.

5.4. Korzystanie z systemów teleinformatycznych poza firmą

- Użytkownicy wyposażeni w sprzęt teleinformatyczny poza biurem muszą podjąć dodatkowe środki ostrożności celem zapewnienia poufności oraz integralności firmowych danych teleinformatycznych:
- odpowiednio zabezpieczać przenośne urządzenia, takie jak laptop, palmtop, telefon typu smartfon itp.,
 - dopilnować, aby sprzęt teleinformatyczny nie był użytkowany bez upoważnienia przez osoby nie będące pracownikami Solaris,
 - zapewnić, aby poufne informacje nie zostały udostępnione osobom trzecim (np. przez podejrzenie korzystając z laptopa w publicznych środkach transportu).

5.5. Korzystanie z poczty elektronicznej i komunikatorów

- 5.5.1. Użytkownicy powinni wykazywać się szczególną ostrożnością komunikując się za pomocą poczty elektronicznej. Wyrażenie faktu, zamiaru i opinii w e-mailu może być wiążące dla użytkownika i/lub Solaris oraz tak jak każdy pisemny dokument może stanowić dowód w sądzie.
- 5.5.2. Do nieformalnej komunikacji użytkownicy powinni posługiwać się wewnętrznymi komunikatorami sieciowymi w miejsce poczty elektronicznej.
- 5.5.3. Użytkownikom nie wolno wysyłać pocztą elektroniczną lub poprzez komunikatory wiadomości lub załączników stanowiących materiały niedozwolone. Dotyczy to również używania przekleństw, czynienia nieprzyzwoitych lub uwłaczających uwag czy komentarzy pod adresem użytkowników, klientów lub innych osób.
- 5.5.4. Użytkownikom nie wolno wysyłać poufnych danych teleinformatycznych przez Internet bez odpowiedniego zabezpieczenia. Wymogiem minimalnym jest zabezpieczenie poufnych danych teleinformatycznych poprzez skompresowanie pliku i zabezpieczenie go hasłem.
- 5.5.5. Użytkownikom poczty elektronicznej i komunikatorów znajdujących się w systemie teleinformatycznym nie wolno świadomie rozpowszechniać lub przysyłać dalej fałszywych ostrzeżeń o wirusach, „łańcuszków szczęścia” lub jakichkolwiek innych nieoczekiwanych masowo rozsyłanych wiadomości.
- 5.5.6. Użytkownikom nie wolno uzyskiwać dostępu do skrzynki odbiorczej lub folderów poczty elektronicznej innej osoby bez wyraźnej zgody zainteresowanej osoby, lub jej przełożonego oraz wysyłać wiadomości rzekomo pochodzących od tej osoby.
- 5.5.7. Użytkownikom nie wolno przysyłać służbowych dokumentów na osobiste konta internetowe oraz wirtualne dyski osobiste. Użytkownicy nie mogą wysyłać poufnych dokumentów na domowe konta poczty elektronicznej. Użytkownik powinien wnioskować o zdalny dostęp do sieci, jeżeli potrzebuje dostępu do teleinformatycznych danych firmowych poza siedzibą firmy. Za zgodą przełożonego niniejszego punktu można nie stosować w nagłych sytuacjach służbowych.
- 5.5.8. Użytkownicy zobowiązani są dochować prywatności członków grupy korespondencyjnej, kiedy członkowie grupy nie są świadomi tożsamości innych adresatów wiadomości (wykorzystanie pola UDW).
- 5.5.9. Dozwolone jest korzystanie jedynie z tych komunikatorów, które zostały zatwierdzone do użytku przez Helpdesk.
- 5.5.10. Z komunikatorów sieciowych do których nie zostały przydzielone uprawnienia nie należy korzystać w celu przekazania informacji poufnych.
- 5.5.11. Za pomocą zewnętrznych komunikatorów nie należy przekazywać poufnych danych osobowych.

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	<u>BUS</u>	<u>TRAM</u>		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 7 z 9

5.5.12. Komunikatory sieciowe służą do natychmiastowego przesyłania nietrwałych wiadomości, których ulotny charakter można porównać do krótkiej rozmowy telefonicznej albo krótkiej bezpośredniej rozmowy.

5.6. Korzystanie z systemów teleinformatycznych - użytek prywatny

- 5.6.1. Mimo, że systemy teleinformatyczne mają służyć do celów służbowych, zezwala się na okazjonalne (sporadyczne) korzystanie z nich dla celów prywatnych pod warunkiem, że będzie ono zgodne z obowiązującymi procedurami i zasadami obowiązującymi w Solaris. Użytkownicy powinni być jednak świadomi, że korzystając z tych zasobów dla celów niesłużbowych należy spodziewać się ograniczonej prywatności. Solaris może monitorować taką komunikację z racji prowadzonego systemu bezpieczeństwa informacji.
- 5.6.2. Pod żadnym pozorem nie wolno użytkownikom korzystać z systemów teleinformatycznych Solaris w związku z własną działalnością gospodarczą.
- 5.6.3. Użytkownicy są zobowiązani zapewnić, że korzystanie ze sprzętu i systemów teleinformatycznych dla celów prywatnych:
- nie koliduje z wykonywaniem przez nich obowiązków służbowych,
 - nie jest traktowane priorytetowo wobec obowiązków służbowych,
 - nie powoduje zwiększenia firmowych kosztów utrzymania danych teleinformatycznych użytkownika,
 - nie wiąże się z zaciąganiem nieuzasadnionych wydatków lub zobowiązań przez Solaris,
 - w żaden sposób nie odbija się negatywnie na Solaris,
 - jest zgodne z prawem oraz procedurami i regulaminami Solaris,
 - nie występuje w nadmiernym stopniu.
- 5.6.4. Użytkownicy muszą być świadomi, że korespondencja powstała przy użyciu elektronicznych systemów teleinformatycznych Solaris (z prywatnymi wiadomościami e-mail włącznie) jest zapisywana na kopiach zapasowych i może być przechowywana bez jakichkolwiek ograniczeń czasowych.
- 5.6.5. Prywatne korzystanie z systemów teleinformatycznych oznacza zgodę na określone przez Solaris warunki ich użytkowania oraz zgodę na monitorowanie przez Solaris prywatnych wiadomości przesyłanych pocztą elektroniczną oraz prywatnych danych teleinformatycznych przechowywanych na komputerze.
- 5.6.6. Pliki osobiste należy zapisywać w pamięci komputerów osobistych. Nie należy przechowywać ich na serwerach sieciowych.

5.7. Korzystanie z Internetu i Intranetu

- 5.7.1. Dane teleinformatyczne identyfikujące komputer użytkownika podczas odwiedzania stron internetowych mogą być rejestrowane. Wszystkie czynności dokonywane przez użytkownika przez Internet przy wykorzystaniu systemów teleinformatycznych Solaris mogą pozostawiać ślad wskazujący na ich dokonanie przez Solaris.
- 5.7.2. Użytkownikom nie wolno umyślnie odwiedzać stron internetowych, które zawierają materiały niedozwolone.
- 5.7.3. Odwiedzając jakąkolwiek stronę internetową użytkownicy zawsze muszą przestrzegać warunków korzystania z danej strony.
- 5.7.4. Użytkownicy powinni być świadomi, że Solaris ma prawo do blokowania dostępu do stron internetowych, które uznaje za niestosowne. Wszelkie próby uzyskania dostępu do takich stron są monitorowane i rejestrowane.

5.8. Monitorowanie komunikacji przez Solaris

- 5.8.1. Solaris jest ostatecznie odpowiedzialny za całość komunikacji biznesowej pracowników korzystających z systemów teleinformatycznych, jednakże w możliwym i stosownym zakresie będzie respektować prywatność i autonomię użytkowników i pracowników podczas pracy.
- 5.8.2. Solaris może monitorować elektroniczną komunikację użytkownika m.in. z następujących powodów:
- dostarczanie dowodów transakcji biznesowych,
 - dopilnowanie przestrzegania procedur, polityk i umów wiążących pracowników,
 - zgodność z wymogami prawnymi, Kodeksem Dobrych Praktyk oraz innymi regulaminami funkcjonującymi w Solaris,

	PROCEDURA			XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris			
	BUS	TRAM	Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego				Strona 8 z 9

- zabezpieczanie, wykrywanie oraz sprawdzanie nieuprawnionego korzystania z systemów teleinformatycznych lub działalności przestępczej,
 - utrzymywanie efektywnego działania systemów teleinformatycznych.
- 5.8.3. Użytkownicy muszą być świadomi, że Solaris będzie monitorować wszystkie e-maile oraz dane teleinformatyczne dotyczące korzystania z systemów teleinformatycznych i sprzętu teleinformatycznego (dotyczy zarówno komunikacji prywatnej, jak i służbowej) z powodów dbania o bezpieczeństwo informacji.
- 5.8.4. Użytkownicy muszą być świadomi, że na skutek monitorowania korespondencji, Solaris może wejść w posiadanie prywatnych informacji o użytkowniku. Na przykład, jeżeli użytkownik regularnie odwiedza strony internetowe konkretnego ugrupowania politycznego lub grupy religijnej, wizyty te mogą wskazywać na poglądy polityczne czy przekonania religijne użytkownika.
- 5.8.5. Użytkowanie systemów teleinformatycznych Solaris do celów prywatnych oznacza zgodę użytkownika na przetwarzanie przez Solaris wszelkich danych teleinformatycznych o charakterze prywatnym, które mogą wyjść na jaw na skutek monitoringu.
- 5.8.6. W uzasadnionych przypadkach koniecznym jest, by Solaris skorzystał z dostępu do wiadomości służbowych użytkownika podczas jego nieobecności, np. podczas zwolnienia chorobowego lub urlopu. Jeżeli ustawienia skrzynki pocztowej użytkownika nie przewidują dostępu do jego skrzynki dla innych uprawnionych osób, dostęp taki będzie udzielony jedynie za zgodą przełożonego.
- 5.8.7. Wszelkie e-maile przechowywane w skrzynce użytkownika, które nie są oznaczone w tytule jako „PRYWATNE”, lub z których opisu w tytule nie wynika w jasny sposób, że mają charakter prywatny, będą traktowane jako wiadomości służbowe. Zapobieganie nieumyślnemu ujawnieniu zawartości prywatnego e-maila poprzez wyraźne oznaczenie wiadomości w tytule leży w gestii Użytkownika.
- 5.8.8. W pewnych okolicznościach Solaris może, przy zachowaniu wszelkich wymogów prawnych, wykorzystać dostęp do firmowej poczty użytkownika.

5.9. Przestrzeganie procedury

- 5.9.1. Nieprzestrzeganie postanowień niniejszej procedury może skutkować wszczęciem postępowania zgodnie z procedurami dyscyplinarnymi obowiązującymi w Solaris oraz zgodnie z zawartymi umowami i obowiązującym prawem.
- 5.9.2. W zależności od okoliczności, kroki te mogą obejmować między innymi wycofanie zgody na korzystanie z systemów teleinformatycznych Solaris dla celów prywatnych, udzielenie upomnienia, nagany lub rozwiązania stosunku pracy z pracownikiem (użytkownikiem) z zastosowaniem okresu wypowiedzenia, ewentualnie ze skutkiem natychmiastowym w szczególności w przypadku stwierdzenia popełnienia przestępstwa, jak również wszelkie prawem dopuszczalne kroki zorientowane na ochronę interesów Solaris, w tym dochodzenie odpowiedniego odszkodowania na drodze postępowania sądowego. Ponadto nieprzestrzeganie postanowień niniejszej procedury może stanowić przestępstwo w świetle przepisów powszechnie obowiązującego prawa.
- 5.9.3. W przypadku powzięcia przez Solaris uzasadnionego podejrzenia o popełnieniu przestępstwa, do właściwych organów zostanie skierowane zawiadomienie o podejrzeniu popełnienia przestępstwa, co w rezultacie może zagrozić osobie naruszającej procedurę surowymi konsekwencjami prawnymi.

VI. Zapisy, ich obieg oraz archiwizacja

6.1. Zapisy dotyczące nadawania uprawnień przechowywane są bezterminowo w wersji elektronicznej

VII. Dokumenty związane

Numer	Nazwa dokumentu
XII-00-00-00	Księga Procesu IT i bezpieczeństwo informacji
	Polityka kopii bezpieczeństwa i archiwizacji danych – dostępna w Dziale IT

VIII. Schematy

Numer	Nazwa załącznika

IX. Załączniki

	PROCEDURA				XII-02-00-00
	Użytkowanie systemów i sprzętu teleinformatycznego w Solaris				
	<u>BUS</u>	<u>TRAM</u>		Edycja 3	03.09.2015
Niniejszy dokument jest własnością SOLARIS Bus & Coach S.A. - wyłącznie do użytku wewnętrznego					Strona 9 z 9

Numer	Nazwa załącznika

X. Zmiany

Edycja	Data	Opis
1	25.02.2008	Wydanie procedury Autor: Grzegorz Gruszecki
2	16.11.2009	Zmiana numeru procedury wcześniej obowiązywał numer XII-02-00 Autor zmiany: Anna Biernacik
3	03.09.2015	1) Całościowe przebudowanie procedury. 2) Zmiana nazwy z „Zarządzanie zasobami informatycznymi” na „Użytkowanie systemów i sprzętu teleinformatycznego w Solaris” 3) Usunięcie załączników XII-02-00-01 - Wniosek o nadanie uprawnień do korzystania z zasobów informatycznych XII-02-00-02 - Wniosek o usunięcie uprawnień do korzystania z zasobów informatycznych XII-02-00-03 - Wykaz oprogramowania XII-02-00-04 - Pliki szczególne XII-02-00-05 - Wykaz osób upoważnionych do przeglądów i konserwacji. 4. W procedurze uwzględniono zapisy z wycofanej procedury XII-01-00 Administrowanie systemem informatycznym Autor zmiany: Maciej Król