

# VS DATA S.C.

z siedzibą w Gdyni

81-391, ul. Świętojańska 55/15

tel. (+48 58) 661 45 28



## KSIĘGA BEZPIECZEŃSTWA INFORMACJI

Egzemplarz nr: 1

Wersja: 1.1

	Opracował	Zatwierdził
Imię i nazwisko	<b>Łukasz Chołyst</b>	<b>Witold Sobolewski</b>
Data	2008.02.20	2008.02.20
Podpis		

Gdynia, 2008.02.20

## SPIS TREŚCI

SPIS TREŚCI .....	2
1.1 Postanowienia ogólne .....	7
1.2 Zastosowanie .....	7
2. POWOŁANIA NORMATYWNE .....	7
3. TERMINY I DEFINICJE .....	7
4. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI) .....	9
4.1 Postanowienia ogólne .....	9
4.2 Ustanowienie i zarządzanie SZBI .....	10
4.2.1 Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) .....	10
4.2.1.1 Zakres SZBI .....	10
4.2.1.2 Polityka bezpieczeństwa informacji .....	11
4.2.1.3 Polityka szacowania ryzyka .....	12
4.2.1.3.1 Metoda szacowania ryzyka .....	13
4.2.1.3.2 Plan postępowania z ryzykiem .....	13
4.2.2 Wdrożenie i stosowanie SZBI .....	13
4.2.3 Monitorowanie i przegląd SZBI .....	14
4.2.4 Utrzymanie i doskonalenie SZBI .....	15
4.3 Wymagania dotyczące dokumentacji .....	15
4.3.1 Postanowienia ogólne .....	15
4.3.2 Nadzór nad dokumentami .....	16
4.3.3 Nadzór nad zapisami .....	16
5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA .....	16
5.1 Zaangażowanie kierownictwa .....	16
5.2 Zarządzanie zasobami .....	17
5.2.1 Zapewnienie zasobów .....	17
5.2.2 Szkolenie, uświadamianie i kompetencje .....	17
6 WEWNĘTRZNE AUDITY SZBI .....	18
7. PRZEGLĄD ZARZĄDZANIA SZBI .....	18
7.1 Postanowienia ogólne .....	18
7.2 Dane wejściowe przeglądu .....	18
7.3 Dane wyjściowe przeglądu .....	19
8 DOSKONALENIE SZBI .....	19
8.1 Ciągłe doskonalenie .....	19
8.2 Działania korygujące .....	19
8.3 Działania zapobiegawcze .....	20
A. CELE STOSOWANIA ZABEZPIECZEŃ I ZABEZPIECZENIA .....	21
A.5 POLITYKA BEZPIECZEŃSTWA .....	21
Cel: A.5.2 Polityka bezpieczeństwa informacji .....	21
Zab: A.5.1.1 Dokument polityki bezpieczeństwa informacji .....	21
Zab: A.5.1.2 Przegląd i ocena .....	21
A.6 ORGANIZACJA BEZPIECZEŃSTWA .....	21
Cel: A.6.2 Wewnętrzna organizacja .....	21
Zab: A.6.1.1 Zaangażowanie kierownictwa w bezpieczeństwo informacji .....	21
Zab: A.6.1.2 Koordynacja bezpieczeństwa informacji .....	22
Zab: A.6.1.3 Alokacja odpowiedzialności związanych z bezpieczeństwem informacji .....	22

Zab: A.6.1.4	Proces autoryzacji urzędów przetwarzających informacje .....	22
Zab: A.6.1.5	Klauzule poufności .....	22
Zab: A.6.1.6	Kontakty z władzami .....	22
Zab: A.6.1.7	Kontakty z grupami specjalnych interesów .....	23
Zab: A.6.1.8	Niezależne przeglądy bezpieczeństwa informacji .....	23
Cel: A.6.2	Strony zewnętrzne .....	23
Zab: A.6.2.1	Identyfikacja ryzyk związanych ze stronami zewnętrznymi .....	23
Zab: A.6.2.2	Spełnianie wymagań bezpieczeństwa w kontaktach z klientami .....	23
Zab: A.6.2.3	Spełnianie wymagań bezpieczeństwa w umowach z osobami trzecimi .....	23
A.7	ZARZĄDZANIE AKTYWAMI .....	23
Cel: A.7.2	Odpowiedzialność za zasoby .....	23
Zab: A.7.1.1	Inwentarz zasobów .....	23
Zab: A.7.1.2	Właścicielstwo zasobów .....	24
Zab: A.7.1.3	Akceptowalne użycie zasobów .....	24
Cel: A.7.2	Klasyfikacja informacji .....	24
Zab: A.7.2.1	Wytyczne do klasyfikacji .....	24
Zab: A.7.2.2	Oznaczanie i postępowanie z informacją .....	24
A.8	BEZPIECZEŃSTWO OSOBOWE .....	24
Cel: A.8.2	Przed zatrudnieniem .....	24
Zab: A.8.1.1	Role i odpowiedzialności .....	24
Zab: A.8.1.2	Sprawdzanie .....	24
Zab: A.8.1.3	Warunki zatrudnienia .....	25
Cel: A.8.2	Podczas zatrudnienia .....	25
Zab: A.8.2.1	Odpowiedzialność kierownictwa .....	25
Zab: A.8.2.2	Świadomość w zakresie bezpieczeństwa informacji, edukacja i szkolenia .....	25
Zab: A.8.2.3	Postępowanie dyscyplinarne .....	26
Cel: A.8.2	Ustanie lub zmiana zatrudnienia .....	26
Zab: A.8.3.1	Odpowiedzialności związane z ustaniem zatrudnienia .....	26
Zab: A.8.3.2	Zwrot zasobów .....	26
Zab: A.8.3.3	Cofnięcie praw dostępu .....	26
A.9	BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE .....	27
Cel: A.9.2	Obszary bezpieczne .....	27
Zab: A.9.1.1	Fizyczna granica obszaru bezpiecznego .....	27
Zab: A.9.1.2	Fizyczne zabezpieczenie wejścia .....	27
Zab: A.9.1.3	Zabezpieczenie biur, pomieszczeń i urzędów .....	27
Zab: A.9.1.4	Zabezpieczenie przed zagrożeniami zewnętrznymi i środowiskowymi .....	27
Zab: A.9.1.5	Praca w obszarach bezpiecznych .....	28
Zab: A.9.1.6	Dostęp publiczny, obszary dostaw i załadunku .....	28
Cel: A.9.2	Zabezpieczenie sprzętu .....	28
Zab: A.9.2.1	Rozmieszczenie sprzętu i jego ochrona .....	28
Zab: A.9.2.2	Urządzenia podtrzymujące .....	28
Zab: A.9.2.3	Bezpieczeństwo okablowania .....	28
Zab: A.9.2.4	Konserwacja sprzętu .....	29
Zab: A.9.2.5	Zabezpieczenie sprzętu poza siedzibą .....	29
Zab: A.9.2.6	Bezpieczne usuwanie sprzętu lub przekazywanie do ponownego użycia .....	29
	W przypadku zmiany właściciela – przekazanie sprzętu dysk jest formatowany, tak aby danych z dysku nie można było odtworzyć i tylko taki sprzęt jest przekazany do nowego właściciela / użytkownika .....	29
Zab: A.9.2.7	Wynoszenie mienia .....	29
A.10	ZARZĄDZANIE KOMUNIKACJĄ I EKSPLOATACJĄ .....	29
Cel: A.10.2	Procedury i odpowiedzialności w zakresie eksploatacji .....	29
Zab: A.10.1.1	Udokumentowane procedury eksploatacji .....	29
Zab: A.10.1.2	Zarządzanie zmianą .....	30
Zab: A.10.1.3	Podział obowiązków .....	30

Zab: A.10.1.4	Oddzielanie urządzeń będących w eksploatacji od przeznaczonych do prac rozwojowych	30
Cel: A.10.2	Zarządzanie dostarczaniem usług przez strony trzecie.....	30
Zab: A.10.2.1	Dostarczanie usług .....	30
Zab: A.10.2.2	Monitorowanie i przegląd usług dostarczanych przez strony trzecie.....	31
Zab: A.10.2.3	Zarządzanie zmianami w usługach świadczonych przez strony trzecie.....	31
Cel: A.10.2	Planowanie i akceptacja systemu.....	31
Zab: A.10.3.1	Zarządzanie pojemnością .....	31
Zab: A.10.3.2	Odbiór systemu.....	31
Cel: A.10.2	Zabezpieczenie przeciwko złośliwemu i mobilnemu oprogramowaniu .....	31
Zab: A.10.4.1	Zabezpieczenie przeciwko złośliwemu oprogramowaniu .....	31
Zab: A.10.4.2	Zabezpieczenie przeciwko mobilnemu oprogramowaniu .....	31
Cel: A.10.2	Kopie zapasowe.....	32
Zab: A.10.5.1	Kopie zapasowe informacji .....	32
Cel: A.10.2	Zarządzanie bezpieczeństwem sieci .....	32
Zab: A.10.6.1	Zabezpieczenia sieci.....	32
Zab: A.10.6.2	Bezpieczeństwo usług sieciowych .....	32
Cel: A.10.2	Postępowanie z nośnikami .....	32
Zab: A.10.7.1	Zarządzanie wymiennymi nośnikami .....	32
Zab: A.10.7.2	Niszczanie nośników.....	32
Zab: A.10.7.3	Procedury postępowania z nośnikami .....	32
Zab: A.10.7.4	Bezpieczeństwo dokumentacji systemu .....	32
Cel: A.10.2	Wymiana informacji.....	33
Zab: A.10.8.1	Polityki i procedury w zakresie wymiany informacji .....	33
Zab: A.10.8.2	Umowy w zakresie wymiany .....	33
Zab: A.10.8.3	Nośniki fizyczne podczas transportu.....	33
Zab: A.10.8.4	Elektroniczne wiadomości.....	33
Zab: A.10.8.5	Systemy informacji biznesowej.....	33
Cel: A.10.2	Bezpieczeństwo handlu elektronicznego.....	34
Zab: A.10.9.1	Handel elektroniczny.....	34
Zab: A.10.9.2	Transakcje on-line.....	34
Zab: A.10.9.3	Publicznie dostępna informacja .....	34
Cel: A.10.2	Monitorowanie.....	34
Zab: A.10.10.1	Logi dla potrzeb auditu.....	34
Zab: A.10.10.2	Monitorowanie użycia systemu .....	34
Zab: A.10.10.3	Zabezpieczenie informacji z logów .....	34
Zab: A.10.10.4	Logi administratora i użytkownika .....	34
Zab: A.10.10.5	Logi błędów .....	35
Zab: A.10.10.6	Synchronizacja zegarów .....	35
A.11	KONTROLA DOSTĘPU.....	35
Cel: A.11.2	Potrzeby biznesowe związane z dostępem do systemu .....	35
Zab: A.11.1.1	Polityka kontroli dostępu .....	35
Cel: A.11.2	Zarządzanie dostępem użytkowników .....	35
Zab: A.11.2.1	Rejestrowanie użytkowników .....	35
Zab: A.11.2.2	Zarządzanie przywilejami.....	35
Zab: A.11.2.3	Zarządzanie hasłami użytkowników .....	35
Zab: A.11.2.4	Przegląd praw dostępu użytkowników .....	36
Cel: A.11.2	Zakres odpowiedzialności użytkowników .....	36
Zab: A.11.3.1	Użycie haseł.....	36
Zab: A.11.3.2	Pozostawianie sprzętu użytkownika bez opieki .....	36
Zab: A.11.3.3	Polityka czystego biurka i ekranu.....	36
Cel: A.11.2	Kontrola dostępu do sieci.....	37
Zab: A.11.4.1	Polityka korzystania z usług sieciowych .....	37
Zab: A.11.4.2	Uwierzytelnianie użytkowników przy połączeniach zewnętrznych .....	37
Zab: A.11.4.3	Identyfikacja urządzeń w sieciach.....	37
Zab: A.11.4.4	Ochrona zdalnych portów diagnostycznych i konfiguracyjnych.....	37
Zab: A.11.4.5	Rozdzielanie sieci .....	37
Zab: A.11.4.6	Kontrola połączeń sieciowych.....	37

Zab: A.11.4.7	Kontrola routingu w sieciach .....	37
Cel: A.11.2	Kontrola dostępu do systemów operacyjnych .....	37
Zab: A.11.5.1	Bezpieczne procedury rejestrowania terminalu w systemie .....	37
Zab: A.11.5.2	Identyfikacja i uwierzytelnianie użytkowników .....	38
Zab: A.11.5.3	System zarządzania hasłami .....	38
Zab: A.11.5.4	Użycie systemowych programów narzędziowych.....	38
Zab: A.11.5.5	Wyłączanie terminalu po określonym czasie nieaktywności .....	38
Zab: A.11.5.6	Ograniczenie czasu trwania połączenia .....	38
Cel: A.11.2	Kontrola dostępu do informacji i aplikacji.....	38
Zab: A.11.6.1	Ograniczenie dostępu do informacji .....	38
Zab: A.11.6.2	Izolowanie systemów wrażliwych.....	39
Cel: A.11.2	Komputery przenośne i praca na odległość.....	39
Zab: A.11.7.1	Przenośne komputery i urządzenia komunikacyjne.....	39
Zab: A.11.7.2	Praca na odległość .....	39
A.12	POZYSKANIE, ROZWÓJ I UTRZYMANIE SYSTEMU .....	39
Cel: A.12.2	Wymagania bezpieczeństwa systemów IT .....	39
Zab: A.12.1.1	Analiza i opis wymagań bezpieczeństwa.....	39
Cel: A.12.2	Prawidłowe przetwarzanie w aplikacjach.....	39
Zab: A.12.2.1	Walidacja danych wejściowych.....	39
Zab: A.12.2.2	Kontrola wewnętrznego przetwarzania .....	39
Zab: A.12.2.3	Uwierzytelnianie wiadomości (integralność).....	40
Zab: A.12.2.4	Walidacja danych wyjściowych .....	40
Cel: A.12.2	Zabezpieczenia kryptograficzne .....	40
Zab: A.12.3.1	Polityka używania zabezpieczeń kryptograficznych .....	40
Zab: A.12.3.2	Zarządzanie kluczami .....	40
Cel: A.12.2	Bezpieczeństwo plików systemowych .....	40
Zab: A.12.4.1	Kontrola eksploatowanego oprogramowania.....	40
Zab: A.12.4.2	Ochrona systemowych danych testowych .....	40
Zab: A.12.4.3	Kontrola dostępu do bibliotek programów źródłowych .....	41
Cel: A.12.2	Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej .....	41
Zab: A.12.5.1	Procedury kontroli zmian .....	41
Zab: A.12.5.2	Przegląd techniczny aplikacji po zmianach w systemie operacyjnym .....	41
Zab: A.12.5.3	Ograniczenie dotyczące zmian w pakietach oprogramowania.....	41
Zab: A.12.5.4	Wyciek informacji .....	41
Zab: A.12.5.5	Prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej .....	41
Cel: A.12.2	Zarządzanie techniczną podatnością na zagrożenia .....	42
Zab: A.12.6.1	Kontrolowanie technicznej podatności na zagrożenia .....	42
A.13	ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI .....	42
Cel: A.13.2	Zgłaszanie zdarzeń i słabości związanych z bezpieczeństwem informacji .....	42
Zab: A.13.1.1	Raportowanie zdarzeń związanych z bezpieczeństwem informacji .....	42
Zab: A.13.1.2	Raportowanie słabości związanych z bezpieczeństwem.....	42
Cel: A.13.2	Zarządzanie incydentami i ulepszeniami związanymi z bezpieczeństwem informacji	42
Zab: A.13.2.1	Odpowiedzialności i procedury .....	42
Zab: A.13.2.2	Nauka z incydentów związanych z bezpieczeństwem informacji .....	42
Zab: A.13.2.3	Zbieranie dowodów .....	43
A.14	ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA .....	43
Cel: A.14.2	Aspekty zarządzania ciągłością działania związane z bezpieczeństwem informacji	43
Zab: A.14.1.1	Włączanie bezpieczeństwa informacji w proces zarządzania ciągłością	43
działania	43	
Zab: A.14.1.2	Ciągłość działania i analiza ryzyka .....	43
Zab: A.14.1.3	Tworzenie i wdrażanie planów ciągłości działania uwzględniających	43
bezpieczeństwo informacji .....	43	
Zab: A.14.1.4	Struktura planowania ciągłości działania .....	44
Zab: A.14.1.5	Testowanie, utrzymywanie i ponowna ocena planów ciągłości działania .....	44

A.15 ZGODNOŚĆ .....	44
Cel: A.15.2    Zgodność z przepisami prawa .....	44
Zab: A.15.1.1    Identyfikacja odpowiednich przepisów prawnych .....	44
Zab: A.15.1.2    Prawo do własności intelektualnej .....	44
Zab: A.15.1.3    Zabezpieczanie zapisów organizacji.....	44
Zab: A.15.1.4    Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych	45
Zab: A.15.1.5    Zapobieganie nadużywaniu urządzeń przetwarzających informacje.....	45
Zab: A.15.1.6    Regulacje dotyczące zabezpieczeń kryptograficznych .....	45
Cel: A.15.2    Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna	45
Zab: A.15.2.1    Zgodność z politykami bezpieczeństwa i standardami .....	45
Zab: A.15.2.2    Sprawdzanie zgodności technicznej .....	45
Cel: A.15.2    Rozważania dotyczące audytu systemu.....	45
Zab: A.15.3.1    Zabezpieczenia audytu systemów IT .....	45
Zab: A.15.3.2    Ochrona narzędzi audytu systemów IT .....	46
ZAPISY .....	46
DOKUMENTY ZWIĄZANE .....	46
HISTORIA ZMIAN DOKUMENTU .....	46

## 1. ZAKRES NORMY

### 1.1 Postanowienia ogólne

Norma międzynarodowa ISO 27001:2005 dotyczy wszystkich rodzajów organizacji (przedsiębiorstw komercyjnych, agencji rządowych, organizacji nie nastawionych na zysk) oraz określa wymagania dotyczące ustanawiania, wdrażania, stosowania, monitorowania, przeglądu, utrzymywania i udoskonalania udokumentowanego SZBI (Systemu Zarządzania Bezpieczeństwem Informacji) w całościowym kontekście ryzyk biznesowych. Wyznacza ona wymagania dotyczące wdrażania zabezpieczeń dostosowanych do potrzeb pojedynczych organizacji lub ich części

Wdrożony w VS DATA SZBI jest zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne VS DATA oraz aby uzyskać zaufanie klienta i innych zainteresowanych stron.

Wdrażając SZBI w VS DATA i ustanawiając zabezpieczenia wykorzystane zostały wytyczne normy ISO/IEC 17799:2005.

### 1.2 Zastosowanie

Wymagania wytyczne w normie ISO 27001:2005 są ogólne i można je stosować we wszystkich organizacjach, niezależnie od rodzaju, wielkości i natury biznesu. Pominięcie jakiegokolwiek wymagania określonego w Klauzulach 4, 5, 6, 7 i 8 nie jest akceptowane w wypadku kiedy organizacja stara się o zgodność z niniejszą normą międzynarodową.

Każde wyłączenia zabezpieczeń, o którego potrzebie zdecydowano na podstawie kryteriów akceptowania ryzyka, należy uzasadnić i temu uzasadnieniu ma towarzyszyć odpowiednie potwierdzenie, że powiązane ryzyka zostały we właściwy sposób zaakceptowane przez osoby odpowiedzialne.

## 2. Powołania normatywne

Wdrożony w VS DATA System Zarządzania Bezpieczeństwem Informacji (SZBI) jest zgodny z międzynarodowymi normami:

- ISO/IEC 27001:2005; Techniki informacyjne — Techniki bezpieczeństwa — System zarządzania bezpieczeństwem informacji — Wymagania
- oraz ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management

## 3. Terminy i definicje

Terminy i definicje zastosowane w niniejszej Księdze oraz innych dokumentach SZBI są zgodne z terminologią stosowaną w normie 27001:2005.

### 3.1 Aktywa

wszystko co posiada wartość dla organizacji

[ISO/IEC 13335-1:2004]

### 3.2 Dostępność

zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy gdy jest to potrzebne

[ISO/IEC 13335-1:2004]

### **3.3 Poufność**

zapewnienie, że informacja jest dostępna tylko dla upoważnionych do tego osób, jednostek lub procesów

[ISO/IEC 13335-1:2004]

### **3.4 Bezpieczeństwo informacji**

bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji, oraz inne właściwości takie jak autentyczność, odpowiedzialność, brak odrzucenia i wiarygodność

[ISO/IEC 17799:2005]

### **3.5 Zdarzenie związane z bezpieczeństwem informacji**

określone wystąpienie pewnego stanu systemu, usługi lub sieci wskazujące na prawdopodobne naruszenie polityki bezpieczeństwa informacji lub awarie zabezpieczeń, lub też wcześniej nie znanej sytuacji, która może być istotna ze względów bezpieczeństwa

[ISO/IEC TR 18044:2004]

### **3.6 Incydent związany z bezpieczeństwem informacji**

pojedyncze wydarzenie bądź seria niepożądanych lub niespodziewanych wydarzeń związanych z bezpieczeństwem, które mogą, z dużym prawdopodobieństwem, zagrażać operacjom związanym z działalnością oraz stanowić zagrożenie dla bezpieczeństwa informacji

[ISO/IEC TR 18044:2004]

### **3.7 System zarządzania bezpieczeństwem informacji SZBI**

ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, stosowania, monitorowania, przeglądania, utrzymywania i udoskonalania bezpieczeństwa informacji

### **3.8 Integralność**

zapewnienie dokładności i kompletności informacji

the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

### **3.9 Ryzyko szczątkowe**

ryzyko pozostałe po zabiegach postępowania z ryzykiem

[ISO/IEC Guide 73:2002]

### **3.10 Akceptowanie ryzyka**

decyzja aby zaakceptować ryzyko

[ISO/IEC Guide 73:2002]

### **3.11 Analiza ryzyka**

systematyczne korzystanie z informacji w celu określenia źródeł i oceny ryzyka

[ISO/IEC Guide 73:2002]

### **3.12 Szacowanie ryzyka**

całościowy proces analizy ryzyka i oceny ryzyka

[ISO/IEC Guide 73:2002]

### **3.13 Ocena ryzyka**

proces porównywania oszacowanego ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka.

[ISO/IEC Guide 73:2002]

### **3.14 Zarządzanie ryzykiem**

skoordynowane działania w celu kierowania i kontroli organizacji z uwzględnieniem ryzyka

[ISO/IEC Guide 73:2002]

### **3.15 Postępowanie z ryzykiem**

proces polegający na wyborze i wdrożeniu środków modyfikujących ryzyko [ISO/IEC Guide 73:2002]

[ISO/IEC Guide 73:2002]

### **3.16 Deklaracja stosowania**

dokument, w którym opisano cele stosowania zabezpieczeń i zabezpieczenia, które odnoszą się i mają zastosowanie w SZBI danej organizacji

## **4. System Zarządzania Bezpieczeństwem Informacji (SZBI)**

### **4.1 Postanowienia ogólne**

Firma VS DATA opracowała, wdrożyła, stosuje, monitoruje, przegląda, utrzymuje i doskonali udokumentowany SZBI w kontekście całościowych działań biznesowych i ryzyka, które występują w organizacji.

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z postanowieniami międzynarodowej normy ISO 27001:2005 jest strategiczną decyzją VS DATA. Zastosowano procesowe podejście dla ustanawiania, wdrażania, stosowania, monitorowania, przeglądania, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Zastosowany proces opiera się na modelu PDCA (Planuj – Działaj – Weryfikuj – Doskonal).

## 4.2 Ustanowienie i zarządzanie SZBI

### 4.2.1 Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

W celu zaspokojenia potrzeb i oczekiwań klientów VS DATA S.C z zachowaniem pełnej gwarancji bezpieczeństwa i poufności przetwarzanych informacji, Właściciele Spółki podjęli decyzję o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji, zgodnego z międzynarodowym standardem ISO 27001:2005 - Zarządzeniem właścicieli VS DATA:

- **nr 1 z dnia 06 listopada 2007 r. w sprawie powołania zespołu ds. wdrożenia zintegrowanego systemu zarządzania jakością i zarządzania bezpieczeństwem informacji. Powołania Przedstawiciela kierownictwa ds. Systemu Zarządzania Jakością i Bezpieczeństwem Informacji.**

#### 4.2.1.1 ZAKRES SZBI

- Ustanowiony i wdrożony w VS DATA System Zarządzania Bezpieczeństwem Informacji zgodny z międzynarodową normą ISO 27001:2005 obejmuje swym zakresem wszelką informację przetwarzaną przez Spółkę

**Z zakresu stosowanych zabezpieczeń SZBI wyłączone zostały niżej wskazane cele stosowania zabezpieczeń i zabezpieczenia:**

Cel: A.10.1 Procedury i odpowiedzialności w zakresie eksploatacji

Zab: A.10.1.4 Oddzielenie urządzeń będących w eksploatacji od przeznaczonych do prac rozwojowych

#### **UZASADNIENIE:**

VS DATA nie prowadzi prac rozwojowych.

Cel. A.10.10. Monitorowanie

Zab A.10.10.1 Dziennik auditu

#### **UZASADNIENIE:**

Nie stosuje się oprogramowania zarządzającego planowaniem i prowadzeniem auditu. Nie tworzone są logi w systemie.

Cel: A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym

Zab: A.10.4.2 Zabezpieczenia przed kodem mobilnym

#### **UZASADNIENIE:**

Oprogramowanie mobilne nie jest dopuszczone do wewnętrznych zasobów informatycznych VS DATA

Cel: A.10.9 Bezpieczeństwo handlu elektronicznego

Zab: A.10.9.1 Handel elektroniczny

Zab: A.10.9.2 Transakcje on-line

#### **UZASADNIENIE:**

VS DATA nie prowadzi działalności w obszarze handlu elektronicznego.

Cel: A.12.3 Zabezpieczenia kryptograficzne

zab: A.12.3.1 Polityka korzystania z zabezpieczeń kryptograficznych

zab: A.12.3.2 Zarządzanie kluczami

#### **UZASADNIENIE:**

VS DATA nie korzysta z zabezpieczeń kryptograficznych.

Cel: A.12.5 Bezpieczeństwo w procesach rozwojowych i obsł. informatycznej

zab: A.12.5.5 Prace rozwojowe nad oprogramowaniem powierzone firmie zewn.

#### **UZASADNIENIE:**

W VS DATA nie występują prace rozwojowe nad wykorzystywanym oprogramowaniem. Wykorzystywane oprogramowanie jest upgradowane z aktualizacji dostępnych na rynku.

Cel: A.15.1 Zgodność

zab: A.15.1.6 Regulacje dot. zabezpieczeń kryptograficznych

#### **UZASADNIENIE:**

VS DATA nie korzysta z zabezpieczeń kryptograficznych

Cel: A.15.3 Rozwiązania dot. auditów systemów informacyjnych

zab: A.15.3.1 Zabezpieczenia auditu systemów IT

zab: A.15.3.2 Dostęp do narzędzi auditu systemów informacyjnych

#### **UZASADNIENIE:**

VS DATA nie korzysta z elektronicznych narzędzi auditów systemów informacyjnych. Audyty przeprowadzane są poprzez bezpośrednią kontrolę stanowiska pracy.

### **4.2.1.2 POLITYKA BEZPIECZEŃSTWA INFORMACJI**

Polityka Bezpieczeństwa Informacji została zatwierdzona przez Właścicieli VS DATA wprowadzona w życie Zarządzeniem nr 1 z dnia 06.11.2007 r. w sprawie zatwierdzenia i rozpowszechnienia Polityki Jakości i Polityki Bezpieczeństwa Informacji VS DATA

#### **Polityka Bezpieczeństwa Informacji VS DATA**

- Jednym z podstawowych celów VS DATA jest:

**”ZASPOKAJANIE POTRZEB I SPEŁNIANIE OCZEKIWAŃ KLIENTÓW W ZAKRESIE ODZYSKIWANIA DANYCH KOMPUTEROWYCH. BEZPIECZNEGO USUWANIA INFORMACJI CYFROWYCH”.**

W celu spełnienia tej deklaracji, Kierownictwo VS DATA przyjęło następującą Politykę Bezpieczeństwa Informacji:

1. Jesteśmy świadomi ważności informacji przetwarzanej w Spółce i będziemy stwarzać warunki, aby zapewnić jej bezpieczeństwo, w tym również poprzez zabezpieczenie na jej ochronę odpowiednich środków finansowych.
2. Zobowiązujemy się do spełnienia wymagań prawnych i kontraktowych związanych z bezpieczeństwem informacji, szczególnie w zakresie przepisów o ochronie danych osobowych.
3. W VS DATA funkcjonuje System Zarządzania Bezpieczeństwem Informacji zgodny z międzynarodowym standardem 27001:2005; zakresem ochrony objęto wszelkie informacje przetwarzane w Spółce w każdej formie i w każdym z miejsc działania VS DATA. Za bezpieczeństwo informacji w VS DATA odpowiada każdy właściciel zasobów na swoim stanowisku pracy; zapewnienie bezpieczeństwa koordynuje Zespół ds. Wdrożenia SZBI.
4. Na podstawie niniejszej Polityki zostały sformułowane poszczególne cele w zakresie bezpieczeństwa informacji, które są realizowane poprzez odpowiednie polityki i inne zabezpieczenia, obejmujące w szczególności:
  - a. zapewnienie wykształcenia i świadomości pracowników w zakresie bezpieczeństwa informacji;
  - b. zapewnienie ciągłości działania Spółki;
  - c. zakomunikowanie pracownikom konsekwencji, w tym dyscyplinarnych, w przypadku naruszenia bezpieczeństwa informacji;
  - d. raportowanie incydentów związanych z bezpieczeństwem informacji.
5. W VS DATA dokonano szacowania ryzyka zgodnie z przyjętą metodą i kryteriami akceptacji ryzyka, opisanymi w Księdze Bezpieczeństwa Informacji, a następnie zaimplementowano w stosunku do zidentyfikowanych ryzyk stosowne zabezpieczenia, zawarte w Planie postępowania z ryzykiem i Deklaracji stosowania. Szacowanie ryzyka będzie stałym elementem naszego działania.
6. Obowiązkiem pracowników Spółki jest przestrzeganie szczegółowych zasad postępowania udokumentowanych w „Księdze Bezpieczeństwa Informacji” oraz wszystkich polityk bezpieczeństwa funkcjonujących w VS DATA.
7. Uczymy się i wyciągamy wnioski z błędów. Będziemy stale doskonalić wdrożony System Zarządzania Bezpieczeństwem Informacji.

Niniejsza Polityka oraz polityki bezpieczeństwa funkcjonujące w Spółce zostały zaakceptowane przez Prezesa oraz zakomunikowane wszystkim pracownikom, którzy zostali zobligowani do ich stosowania.

Nad przestrzeganiem Polityki czuwa osobiście Przedstawiciel Kierownictwa ds. ZSZ

Dokument Polityki Bezpieczeństwa Informacji został zakomunikowany wszystkim pracownikom Spółki oraz zainteresowanym stronom zewnętrznym. Zastosowane formy komunikacji: publikacja Polityki na stronie internetowej [www.vsdata.pl](http://www.vsdata.pl), wywieszenie Polityki na ścianach Spółki, odprawy, szkolenia, audyty wewnętrzne.

#### **4.2.1.3 POLITYKA SZACOWANIA RYZYKA**

Polityka szacowania ryzyka związanego z bezpieczeństwem informacji stanowi odrębny dokument związany z niniejszą Księgą - SZBI\_Pol\_01\_SzacowanieRyzyka\_2008-02-19. Polityka zawiera metodologię szacowania ryzyka oraz podejście do szacowania ryzyka z uwzględnieniem bezpieczeństwa informacji w kontekście biznesowym oraz wymagań prawnych.

Celem Polityki szacowania ryzyka jest zapewnienie, że metodyka szacowania ryzyka przyjęta w VS DATA jest spójna ze zidentyfikowanymi wymaganiami biznesowymi i prawnymi w zakresie ochrony bezpieczeństwa informacji, zawiera kryteria akceptacji ryzyka i że zapewnia uzyskanie porównywalnych wyników w całej organizacji podczas kolejnych szacowań ryzyka.

Załącznikami do dokumentu Polityki szacowania ryzyka są: raport z szacowania ryzyka, Wykaz aktywów; Plan Postępowania Z Ryzykiem, Deklaracja stosowania zabezpieczeń.

#### **4.2.1.3.1 Metoda szacowania ryzyka.**

Metoda szacowania ryzyka jest opisana w Polityce szacowania ryzyka. Zespół ds. Wdrożenia SZBI ustala i zatwierdza metodykę szacowania ryzyka, która jest odpowiednia dla Spółki w kontekście wymagań biznesowych i prawnych związanych z bezpieczeństwem informacji. Metodyka ta powinna zapewnić jednolite rozumienie, w obrębie całej organizacji, wszelkich skal ocen i kryteriów przyjętych podczas szacowania ryzyka i uzyskanie porównywalnych wyników w całej organizacji podczas kolejnych szacowań ryzyka. Metodyka zawiera również kryteria akceptacji ryzyka. Metodyka zawarta jest w pliku SzacowanieRyzyka, szczególnie w arkuszu Metodyka.

#### **4.2.1.3.2 Plan postępowania z ryzykiem**

Na podstawie wyników szacowania ryzyka oraz Deklaracji Stosowania tworzony jest Plan postępowania z ryzykiem. Plan Postępowania z Ryzykiem zawiera:

- działania, które należy podjąć w związku ze zidentyfikowanym i ocenionym ryzykiem (wdrożenie zabezpieczeń),
- zasoby potrzebne do wdrożenia Planu,
- odpowiedzialności, priorytety i terminy wdrożenia poszczególnych elementów Planu.

Wyniki szacowania ryzyka (pliki: Szacowanie Ryzyka, Deklaracja Stosowania, Plan Postępowania Z Ryzykiem) Zespół ds. wdrożenia SZBI przedstawia Kierownictwu organizacji podczas najbliższego przeglądu zarządzania po to, aby Kierownictwo:

- zaakceptowało pozostałe ryzyko (szczątkowe),
- zaakceptowało wyniki szacowania ryzyka i proponowany Plan Postępowania z Ryzykiem.

Działania zawarte w Planie Postępowania z Ryzykiem przekazywane są wymienionym w nim osobom do wdrożenia.

#### **4.2.2 Wdrożenie i stosowanie SZBI**

W celu skutecznego wdrożenia i stosowania SZBI organizacja podjęła następujące działania:

- a) Sformułowała plan postępowania z ryzykiem, w którym są określone odpowiednie działania kierownictwa, zakresy odpowiedzialności oraz priorytety dla zarządzania ryzykami związanymi z bezpieczeństwem informacji.
- b) Wdrożyła plan postępowania z ryzykiem w celu osiągnięcia zidentyfikowanych celów stosowania zabezpieczeń, które obejmują rozważenie finansowania oraz przydzielania ról i zakresów odpowiedzialności.
- c) Wdrożyła zabezpieczenia wymagane w Załączniku A normy ISO 27001:2005 tak, aby osiągnąć cele stosowania zabezpieczeń.

- d) Zdefiniowała w jaki sposób będą odbywać się pomiary skuteczności wybranych zabezpieczeń lub grup zabezpieczeń i sprecyzowała w jaki sposób należy dokonywać pomiarów do oceny skuteczności zabezpieczeń w celu dostarczenia porównywalnych i odtwarzalnych rezultatów.
- e) Wdrożyła programy uświadamiania i szkolenia.
- f) Zarządza stosowaniem SZBI.
- g) Zarządza zasobami SZBI.
- h) Wdraża procedury i inne zabezpieczenia zdolne do zapewnienia natychmiastowego wykrycia i reakcji na incydenty związane z naruszeniem bezpieczeństwa.

#### 4.2.3 Monitorowanie i przegląd SZBI

Organizacja podjęła następujące działania:

- a) Monitoruje, dokonuje przeglądy i stosuje inne środki w celu:
  - 1) natychmiastowego wykrywania błędów w wynikach przetwarzania;
  - 2) natychmiastowego identyfikowania naruszenia bezpieczeństwa oraz incydentów zakończonych niepowodzeniem lub sukcesem;
  - 3) umożliwienia kierownictwu stwierdzenia czy działania związane z bezpieczeństwem delegowane na poszczególne osoby lub wdrożone za pomocą środków informatycznych są wykonywane zgodnie z oczekiwaniami;
  - 4) pomocy w wykryciu działań podejmowanych w celu rozwiązywania problemów związanych z naruszeniem bezpieczeństwa przy uwzględnieniu wskaźników; oraz
  - 5) określenia czy działania podjęte w celu usunięcia problemu były skuteczne.
- b) Wykonuje regularne przeglądy skuteczności SZBI (w tym zgodność z polityką i celami oraz przegląd zabezpieczeń), biorąc pod uwagę wyniki auditów bezpieczeństwa, incydentów, sugestii oraz informacji zwrotnych od wszystkich zainteresowanych stron.
- c) Mierzy skuteczność stosowanych zabezpieczeń w celu określenia czy wymagania dotyczące bezpieczeństwa zostały spełnione.
- d) Dokonuje przeglądy szacowania ryzyka w zaplanowanych przedziałach czasowych. Dokonuje przeglądy ryzyka szacunkowego i akceptowalnego biorąc pod uwagę zmiany:
  - 1) w organizacji;
  - 2) w technologii;
  - 3) celów biznesowych i procesów;
  - 4) zidentyfikowanych zagrożeń;
  - 5) skuteczności zastosowanych zabezpieczeń; oraz
  - 6) zewnętrznych zdarzeń takich jak zmiany prawa lub stosownych regulacji oraz zmiany o charakterze społecznym.
- e) W zaplanowanych odstępach czasu przeprowadza audyty wewnętrzne.
- f) W regularnych odstępach czasu podejmuje przeglądy realizowane przez kierownictwo (co najmniej raz w roku), tak aby zapewnić, że zakres Systemu jest

odpowiedni oraz, że zostały zidentyfikowane udoskonalenia procesów realizowanych w ramach SZBI.

- g) Uaktualnia plany dotyczące bezpieczeństwa, zwracając uwagę na rezultaty z działań monitoringowych i przeglądów.
- h) Rejestruje działania i zdarzenia, które mogą mieć wpływ na skuteczność lub jakość realizacji SZBI.

Pomiar skuteczności wdrożonych zabezpieczeń odbywa się w sposób następujący:

- a) Zespół ds. Wdrożenia SZBI na przeglądach zarządzania ustala skuteczność jakich zabezpieczeń i w jaki sposób będzie mierzona.
- b) Sposób pomiaru, częstotliwość, osoby odpowiedzialne i wyniki pomiarów zapisane są w pliku SzacowanieRyzyka.
- c) Raport na temat skuteczności wdrożonych zabezpieczeń przedstawiany jest przez Zespół ds. Wdrożenia SZBI na przeglądach zarządzania.
- d) W przypadku wykrycia, że zabezpieczenia nie są skuteczne, Zespół ds. Wdrożenia SZBI podejmuje stosowne działania korygujące.

#### **4.2.4 Utrzymanie i doskonalenie SZBI**

W celu utrzymania i doskonalenie SZBI organizacja podjęła następujące działania:

- a) Wdraża w SZBI zidentyfikowane udoskonalenia.
- b) Podejmuje odpowiednie działania korygujące i zapobiegawcze. Wyciąga wnioski z doświadczeń w dziedzinie bezpieczeństwa zarówno innych organizacji, jak i własnej.
- c) Informuje o wynikach działań i uzgadnia je ze wszystkimi zainteresowanymi stronami. Poziom szczegółowości zależy od okoliczności. Jeśli jest to wymagane uzgadnia sposób dalszego postępowania.
- d) Zapewnia, że udoskonalenia osiągają zamierzone cele.

### **4.3 Wymagania dotyczące dokumentacji**

#### **4.3.1 Postanowienia ogólne**

Dokumentacja SZBI zawiera zapisy decyzji kierownictwa, zapewnia o tym, że podejmowane akcje są identyfikowalne do decyzji kierownictwa i polityk, oraz zapewnia, że zapisane rezultaty są odtwarzalne.

Istotną kwestią jest to, żeby organizacja była w stanie zademonstrować związek pomiędzy wybranymi zabezpieczeniami aż do wyników procesu szacowania ryzyka i postępowania z ryzykiem, a w dalszej kolejności do polityki i celów SZBI.

Dokumentacja SZBI VS DATA zawiera:

- a) udokumentowane deklaracje polityki i celów SZBI;
- b) zakres SZBI;
- c) procedury i zabezpieczenia służące realizacji SZBI;
- d) opis metodologii szacowania ryzyka;
- e) SzacowanieRyzyka;
- f) plan postępowania z ryzykiem;

- g) udokumentowane procedury potrzebne organizacji do zapewnienia efektywnego planowania, stosowania i sterowania jej procesami bezpieczeństwa informacji;
- h) zapisy wymagane przez międzynarodową normę ISO 27001:2005 oraz przez organizację w celu spełnienia wymagań;
- i) deklarację stosowania zabezpieczeń.

#### **4.3.2 Nadzór nad dokumentami**

Dokumenty wymagane przez SZBI są chronione i nadzorowane. Zasady nadzoru nad dokumentami SZBI zawarte są w udokumentowanej Procedurze PR5-1 Nadzór nad dokumentami i zapisami, która określa działania kierownictwa potrzebne do:

- a) zatwierdzenia odpowiednich dokumentów przed ich wydaniem;
- b) przeglądu i aktualizacji dokumentów w razie potrzeby oraz ponownego ich zatwierdzenia;
- c) zapewnienia, że zidentyfikowano zmiany i aktualny status zmian dokumentów;
- d) zapewnienia, że najnowsze wersje odpowiednich dokumentów są dostępne w miejscach ich stosowania;
- e) zapewnienia, że dokumenty pozostają czytelne i łatwe do zidentyfikowania;
- f) zapewnienia, że dokumenty są dostępne dla wszystkich, którzy ich potrzebują, że są przekazywane, przechowywane i w końcu niszczone zgodnie z procedurami odpowiednimi do ich klasyfikacji;
- g) zapewnienia, że dokumenty zewnętrzne są identyfikowane;
- h) zapewnienia, że rozpowszechnianie dokumentów jest kontrolowane;
- i) zapobiegania niezamierzonemu stosowaniu nieaktualnych dokumentów; oraz
- j) zastosowania odpowiedniej ich identyfikacji, jeżeli są zachowane z jakichkolwiek powodów.

#### **4.3.3 Nadzór nad zapisami**

W celu dostarczenia świadectwa potwierdzającego zgodność z wymaganiami oraz skutecznego stosowania SZBI zostały ustanowione i utrzymane odpowiednie zapisy. Zapisy te są chronione i nadzorowane. SZBI uwzględnia wszystkie odpowiednie wymagania przepisów prawnych lub regulacyjnych i zobowiązań wynikających z umów. Zapisy pozostają czytelne, łatwe do zidentyfikowania i odtwarzalne. Zabezpieczenia służące identyfikowaniu, przechowywaniu, ochronie, odtwarzaniu, archiwizacji oraz niszczeniu zapisów, zostały udokumentowane.

Zachowane będą zapisy wydajności procesów oraz wszystkie wystąpienia istotnych incydentów związanych z bezpieczeństwem dotyczących SZBI. Przykładami zapisów są raporty z auditu i autoryzacji dostępu, rejestry itp.

Zasady nadzoru nad zapisami reguluje Procedura PR5-1 Nadzór nad dokumentami i zapisami.

## **5 Odpowiedzialność kierownictwa**

### **5.1 Zaangażowanie kierownictwa**

Kierownictwo zapewnia świadectwo swojego zaangażowania w ustanowienie, stosowanie, monitorowanie, przegląd, utrzymanie i doskonalenie SZBI przez:

- a) ustanowienie polityki bezpieczeństwa informacji;
- b) zapewnienie, że cele bezpieczeństwa informacji i plany zostały ustanowione;
- c) określenie ról i zakresów odpowiedzialności w odniesieniu do bezpieczeństwa informacji;
- d) informowanie organizacji o znaczeniu spełniania celów bezpieczeństwa informacji i zgodności z polityką bezpieczeństwa informacji, swojej odpowiedzialności prawnej oraz potrzeby ciągłego doskonalenia;
- e) zapewnienia wystarczających zasobów do opracowania, wdrażania, stosowania, monitorowania, przeglądu, utrzymania i doskonalenia SZBI;
- f) decydowanie o akceptowalnym poziomie ryzyka;
- g) przeprowadzanie przeglądów SZBI realizowanych przez kierownictwo;
- h) przeprowadzanie przeglądów zarządzania SZBI.

## **5.2 Zarządzanie zasobami**

### **5.2.1 Zapewnienie zasobów**

Organizacja określa i zapewnia zasoby potrzebne do:

- a) ustanowienia, stosowania, monitorowania, przeglądu, utrzymania i doskonalenia SZBI;
- b) zapewnienia, że procedury bezpieczeństwa informacji wspomagają wymagania biznesowe;
- c) zidentyfikowanie i odniesienie do wymagań przepisów prawa i wymagań regulacyjnych oraz zobowiązań umownych związanych z bezpieczeństwem;
- d) utrzymania odpowiedniego bezpieczeństwa przez poprawne zastosowanie wszelkich wdrażanych zabezpieczeń;
- e) przeprowadzanie przeglądów, kiedy zachodzi taka potrzeba, oraz odpowiedniego reagowania na wyniki z takich przeglądów; i
- f) poprawy skuteczności SZBI tam gdzie jest to wymagane.

### **5.2.2 Szkolenie, uświadamianie i kompetencje**

Organizacja zapewnia, że cały personel, któremu przypisano zakresy obowiązków określone w SZBI, ma kompetencje do realizacji wymaganych zadań przez:

- a) określenie koniecznych kompetencji personelu wykonującego prace mające wpływ na SZBI;
- b) zapewnienie szkolenia, lub jeśli jest to konieczne, zatrudnienie kompetentnego personelu do realizacji tych potrzeb;
- c) ocenę skuteczności podjętych działań; i
- d) prowadzenie zapisów dotyczących edukacji, szkolenia, umiejętności, doświadczenia i kwalifikacji.

Organizacja zapewni także, żeby cały odpowiedni personel był świadomy związku i znaczenia swoich działań dotyczących bezpieczeństwa informacji oraz wkładu do osiągnięcia celów SZBI.

## 6 Wewnętrzne audyty SZBI

Organizacja planuje wewnętrzne audyty SZBI i przeprowadza przeglądy SZBI w zaplanowanych odstępach czasu w celu określenia czy cele stosowania zabezpieczeń, zabezpieczenia, procesy i procedury SZBI są:

- a) zgodne z wymaganiami międzynarodowej normy 27001:2005, odpowiednimi przepisami prawnymi i wymaganiami o charakterze regulacyjnym;
- b) zgodne z określonymi wymaganiami bezpieczeństwa informacji;
- c) skutecznie wdrażane i utrzymywane;
- d) realizowane w oczekiwany sposób.

Program auditu jest zaplanowany, z uwzględnieniem statusu i znaczenia procesów i obszarów, które będą auditowane, jak również wyników wcześniejszych auditów. Zdefiniowane zostają kryteria i zakres auditu oraz jego częstotliwość i metody. Zarówno wybór auditorów, jak i przeprowadzenie auditu odzwierciedlają obiektywizm i bezstronność procesu auditowego. Audytorzy nie powinni auditować swojej pracy.

Zakres odpowiedzialności i wymagania dotyczące planowania i przeprowadzania auditów oraz zapisywania wniosków i przechowywania zapisów zostały określone w udokumentowanej Procedurze PR4-2 Audyty wewnętrzne.

Kierownictwo odpowiedzialne za auditowany obszar upewnia się, że działania poauditowe są podejmowane bez nieuzasadnionych opóźnień, w celu wyeliminowania wykrytych niezgodności i ich przyczyn. Czynności poauditowe obejmują weryfikację podjętych działań i zapisy z wyników weryfikacji.

## 7. Przegląd zarządzania SZBI

### 7.1 Postanowienia ogólne

Kierownictwo przeprowadza przeglądy zarządzania SZBI w zaplanowanych odstępach czasu w celu zapewnienia jego ciągłej przydatności, adekwatności i skuteczności. Przegląd zawiera ocenę możliwości doskonalenia i potrzeby zmian w SZBI, w tym polityki bezpieczeństwa i celów bezpieczeństwa. Wyniki przeglądów są udokumentowane, a odpowiednie zapisy są przechowywane.

Zakres odpowiedzialności i zasady planowania i przeprowadzania przeglądów zarządzania SZBI zostały określone w udokumentowanej Procedurze PR4-1 Przegląd Zarządzania wykonywany przez Właścicieli.

### 7.2 Dane wejściowe przeglądu

Dane wejściowe do przeglądu zarządzania SZBI zawierają informacje dotyczące:

- a) wyników auditów i przeglądów SZBI;
- b) informacji zwrotnych od zainteresowanych stron;
- c) technik, produktów i procedur, które mogłyby być zastosowane w organizacji w celu ulepszania realizacji i skuteczności SZBI;

- d) statusu działań korygujących i zapobiegawczych w odniesieniu do SZBI;
- e) podatności, lub zagrożeń, do których nie było odpowiedniego odniesienia w poprzednim oszacowaniu ryzyka;
- f) rezultaty pomiarów skuteczności;
- g) działań podjętych na skutek poprzednich przeglądów zarządu;
- h) jakichkolwiek zmian, które mogłyby dotyczyć SZBI; i
- i) zaleceń dotyczących doskonalenia.

### **7.3 Dane wyjściowe przeglądu**

Dane wyjściowe z przeglądu zarządzania SZBI zawierają wszystkie decyzje i działania związane z:

- a) Doskonaleniem skuteczności SZBI;
- b) Aktualizowaniem planu szacowania ryzyka i postępowania z ryzykiem;
- c) Modyfikacją procedur dotyczących bezpieczeństwa informacji, jeśli jest to konieczne, w celu reakcji na wewnętrzne lub zewnętrzne zdarzenia, które mogą mieć konsekwencje dla SZBI, w tym zmiany:
  - 1) wymagań biznesowych;
  - 2) wymagań bezpieczeństwa;
  - 3) procesów biznesowych mających wpływ na istniejące wymagania biznesowe;
  - 4) uwarunkowań prawnych, lub regulacyjnych;
  - 5) zobowiązań umownych;
  - 6) poziomów ryzyka i/lub kryteriów akceptacji ryzyka.
- d) Potrzebnymi zasobami;
- e) Doskonaleniem pomiarów skuteczności stosowanych zabezpieczeń.

## **8 Doskonalenie SZBI**

### **8.1 Ciągłe doskonalenie**

Organizacja w sposób ciągły poprawia skuteczność SZBI przez stosowanie polityki bezpieczeństwa informacji, celów bezpieczeństwa, wyników auditu, analiz monitorowanych zdarzeń, działań korygujących i zapobiegawczych i przeglądów zarządzania.

### **8.2 Działania korygujące**

Organizacja podejmuje działania w celu wyeliminowania przyczyny niezgodności związanych z wdrożeniem i stosowaniem SZBI, tak aby przeciwdziałać powtórny wystąpieniom tych niezgodności. Udokumentowana Procedura PR4-4 Działania korygujące i zapobiegawcze określa wymagania dotyczące:

- a) zidentyfikowania niezgodności;
- b) stwierdzenia przyczyn niezgodności;

- c) oceny potrzeby działań w celu zapewnienia, że niezgodności nie powtórzą się;
- d) wskazania i wdrożenia potrzebnych działań korygujących;
- e) wprowadzenia do dokumentacji zapisów rezultatów podjętych działań;
- f) przeglądu podjętych działań korygujących.

### **8.3 Działania zapobiegawcze**

Organizacja wskazuje działania podejmowane w celu ochrony przed potencjalnymi niezgodnościami z wymaganiami SZBI tak, aby przeciwdziałać ich wystąpieniu. Podejmowane działania zapobiegawcze są dostosowane do wagi potencjalnych problemów. Udokumentowana Procedura PR4-4 Działania korygujące i zapobiegawcze określa wymagania dotyczące:

- a) zidentyfikowania potencjalnych niezgodności i ich przyczyn;
- b) oceny potrzeby działań w celu zapewnienia, że niezgodności nie powtórzą się
- c) wskazania i wdrożenia potrzebnych działań zapobiegawczych;
- d) wprowadzenia do dokumentacji zapisów rezultatów podjętych działań;
- e) przeglądu podjętych działań zapobiegawczych.

Organizacja identyfikuje zmienione ryzyka i zapewnia, że uwaga skoncentruje się na znacząco zmienionych ryzykach. Priorytety działań zapobiegawczych są wskazywane na podstawie szacowania ryzyka.

## **A. Cele stosowania zabezpieczeń i zabezpieczenia.**

Odpowiednie cele stosowania zabezpieczeń oraz zabezpieczenia są wybrane i wdrożone tak, aby spełniały wymagania określone przez oszacowanie ryzyka i proces postępowania z ryzykiem. Wybór jest uzasadniony kryteriami akceptowania ryzyka, jak również wymaganiami prawnymi, regulacyjnymi i wynikającymi z umów.

Cele zabezpieczeń i zabezpieczenia z Załącznika A normy ISO 27001:2005 zostały wybrane jako część procesu szacowania i postępowania z ryzykiem tak, aby odpowiadały określonym wymogom.

### **A.5 Polityka bezpieczeństwa**

**Cel: A.5.2 Polityka bezpieczeństwa informacji**

**Zab: A.5.1.1 Dokument polityki bezpieczeństwa informacji**

Dokument Polityki Bezpieczeństwa Informacji został zatwierdzony przez Właścicieli VS DATA i wprowadzony w życie Zarządzeniem nr 1 z dnia 06.11.2007 r. w sprawie zatwierdzenia i rozpowszechnienia Polityki Jakości i Polityki Bezpieczeństwa Informacji w VS DATA.

**Zab: A.5.1.2 Przegląd i ocena**

Dokument Polityki Bezpieczeństwa Informacji jest poddawany okresowym przeglądom i ocenie co do jej adekwatności i skuteczności. Przegląd i ocena Polityki Bezpieczeństwa Informacji dokonywane są na przeglądzie zarządzania Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji.

### **A.6 Organizacja bezpieczeństwa**

**Cel: A.6.2 Wewnętrzna organizacja**

**Zab: A.6.1.1 Zaangażowanie kierownictwa w bezpieczeństwo informacji**

Właściciele VS DATA S.C w dniu 06.11.2007 podjęli decyzję o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji i zintegrowaniu go z Systemem Zarządzania Jakością.

W związku z powyższym wolą Właścicieli został powołany Zespół ds. Wdrożenia SZBI odpowiedzialny za wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji i zintegrowanie go z Systemem Zarządzania Jakością – Zarządzenie nr 1 z dnia 06.11.2007 w sprawie wdrożenia zintegrowanego Systemu Zarządzania Jakością i Zarządzania Bezpieczeństwem Informacji.

W dniu 5.03.2008 Właściciele VS DATA S.C wydali:

- Zarządzenie nr 2 w sprawie wdrożenia Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji w VS DATA S.C – z dniem 20.02.2008 w VS DATA oficjalnie zaczyna funkcjonować Zintegrowany System Zarządzania Jakością i Bezpieczeństwem Informacji zgodny z międzynarodowymi normami ISO 9001:2000 i

27001:2005, oraz zostaje wprowadzony w życie dokument Polityki Bezpieczeństwa Informacji;

Od 06.11.2007 do 20.02.2008 trwały prace wdrożeniowe nad Systemem, czego efektem jest wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z międzynarodową normą ISO 27001:2005i zintegrowanie go z Systemem Zarządzania Jakością zgodnego z międzynarodową normą ISO 9001:2000.- tworząc Zintegrowany System Zarządzania Jakością i Bezpieczeństwem Informacji funkcjonujący w VS DATA.

#### **Zab: A.6.1.2 Koordynacja bezpieczeństwa informacji**

W celu zapewnienia koordynacji bezpieczeństwa informacji został powołany Zespół ds. Wdrożenia SZBI i konsultantów zewnętrznych.

Zespół odpowiada za określenie / szacowanie i klasyfikację ryzyka związanego z bezpieczeństwem informacji, wybór i przegląd zabezpieczeń oraz utrzymanie i skuteczne funkcjonowanie Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji.

#### **Zab: A.6.1.3 Alokacja odpowiedzialności związanych z bezpieczeństwem informacji**

Odpowiedzialności związane z bezpieczeństwem informacji zapisane są w stanowiskowych kartach pracy, zakresach obowiązków, uprawnień i odpowiedzialności pracowników VS DATA, zarządzeniach Właścicieli Spółki, Politykach SZBI, procedurach ZSZJ i BI, oraz Księdze Bezpieczeństwa Informacji.

#### **Zab: A.6.1.4 Proces autoryzacji urządzeń przetwarzających informacje**

W VS DATA jest ustalona procedura autoryzacji urządzeń przetwarzających informacje, zgodnie z którą wszystkie urządzenia do przetwarzania informacji posiada VS DATA.

ST nadzoruje zakup sprzętu / urządzeń lub ich podzespołów i części, składa sprzęt z dostarczonych elementów, instaluje oprogramowanie i wydaje do użytkowników sprzęt / urządzenia przetwarzające informacje.

Charakterystyka zestawu ujęta jest na „Zestawieniu zbiorczym dla zestawu”, które podpisywane jest przez użytkownika. Rejestr Zestawień w formie elektronicznej i papierowej prowadzony jest przez PJ.

Procedura autoryzacji urządzeń przetwarzających informacje przez ST zawarta jest także w Procedurach ZSZJ i BI: Procedura PR2-2 Zakupy, PR3-1 Zarządzanie infrastrukturą, środowiskiem pracy oraz nadzór nad wyposażeniem do monitorowania i pomiarów.

#### **Zab: A.6.1.5 Klauzule poufności**

Klauzule poufności dotyczące bezpieczeństwa informacji przetwarzanych przez Spółkę, są stosowane we wszystkich umowach cywilno – prawnych zawieranych przez VS DATA

#### **Zab: A.6.1.6 Kontakty z władzami**

VS DATA utrzymuje właściwe kontakty z władzami szczebla lokalnego, regionu i centralnego z racji pełnionych funkcji.

### **Zab: A.6.1.7 Kontakty z grupami specjalnych interesów**

Członkowie Zespołu ds. Wdrożenia SZBI utrzymują stałe kontakty ze specjalistami w zakresie bezpieczeństwa informacji, biorą udział w szkoleniach, seminariach i sympozjach dotyczących bezpieczeństwa informacji.

### **Zab: A.6.1.8 Niezależne przeglądy bezpieczeństwa informacji**

Niezależne przeglądy bezpieczeństwa informacji przeprowadzane są dla każdego zasobu i lokalizacji raz w roku lub częściej w przypadku istotnych zmian organizacyjno-technicznych mających wpływ na bezpieczeństwo informacji.

Przegląd bezpieczeństwa informacji dokonywany jest w trakcie auditów wewnętrznych lub zewnętrznych SZBI oraz poprzez analizę skuteczności stosowanych zabezpieczeń, analizę incydentów i słabości/podatności systemu.

Wnioski z przeglądu bezpieczeństwa informacji prezentowane są na przeglądzie zarządzania ZSZJ i BI.

## **Cel: A.6.2 Strony zewnętrzne**

### **Zab: A.6.2.1 Identyfikacja ryzyk związanych ze stronami zewnętrznymi**

Ryzyka dotyczące bezpieczeństwa informacji związane ze stronami zewnętrznymi zostały określone w Szacowaniu Ryzyka oraz Deklaracji Stosowania Zabezpieczeń SZBI i Planie Postępowania z Ryzykiem. Przed udzieleniem dostępu należy wdrożyć odpowiednie zabezpieczenia.

### **Zab: A.6.2.2 Spełnianie wymagań bezpieczeństwa w kontaktach z klientami**

Przed udzieleniem klientom dostępu do zasobów informacyjnych organizacji wdrożyła odpowiednie zabezpieczenia w celu zapewnienia bezpieczeństwa informacji. Zabezpieczenia mogą mieć formę bezpośredniego nadzoru pracownika Spółki, zapisów w umowach dotyczących bezpieczeństwa informacji i aktywów organizacji (klauzule poufności, zobowiązania, odpowiedzialności, itp.) w zależności od sytuacji i wagi informacji.

### **Zab: A.6.2.3 Spełnianie wymagań bezpieczeństwa w umowach z osobami trzecimi**

Umowy umożliwiające dostęp osób trzecich do urządzeń służących do przetwarzania, przekazywania lub zarządzania informacjami organizacji lub urządzeniami przetwarzającymi informacje, bazuje na formalnych zapisach zawierających wszystkie istotne wymogi bezpieczeństwa. Generalną zasadą jest stosowanie klauzul poufności oraz ściśle określonych zasad dostępu do zasobów organizacji.

## **A.7 Zarządzanie aktywami**

### **Cel: A.7.2 Odpowiedzialność za zasoby**

#### **Zab: A.7.1.1 Inwentarz zasobów**

Wszystkie ważne aktywa z punktu widzenia bezpieczeństwa informacji zostały zinwentaryzowane wg lokalizacji i użytkownika. Zestawienie zbiorcze inwentaryzacji zawiera dokument Wykaz Aktywów. Rejestr ten jest prowadzony i okresowo aktualizowany przez ST.

### **Zab: A.7.1.2 Właścicielstwo zasobów**

Wszystkie zasoby informacyjne oraz aktywa związane z przetwarzaniem informacji mają swoich właścicieli, tj. osoby lub komórki organizacyjne odpowiedzialne za dany zasób lub aktywa. Zasady właścicielstwa i korzystania z komputerów są zawarte w Wykazie Aktywów.

### **Zab: A.7.1.3 Akceptowalne użycie zasobów**

Zasady możliwego do zaakceptowania korzystania z zasobów informacyjnych i aktywów związanych z przetwarzaniem informacji są określone w politykach SZBI, stanowiskowych kartach pracy, upoważnieniach, Zarządzeniach WŁ VS DATA S.C oraz procedurach.

## **Cel: A.7.2 Klasyfikacja informacji**

### **Zab: A.7.2.1 Wytyczne do klasyfikacji**

Wszelka informacja przetwarzana w VS DATA została sklasyfikowana wg 3 grup biorąc pod uwagę swoją wartość, przepisy prawne, stopień wrażliwości i wagę dla organizacji. Grupy informacji:

1. informacje niejawne (**zastrzeżone**, poufne, tajne) - wynikają z Ustawy o ochronie informacji niejawnych;
2. informacje wrażliwe (dane osobowe, dane klienta, dane finansowo-księgowo, dane dotyczące wydawanych decyzji, logi, kopie bezpieczeństwa, itp.);
3. informacje jawne (mało wrażliwe, których ujawnienie / utrata nie spowoduje przerwy w działalności VS DATA S.C i roszczeń stron trzecich).

### **Zab: A.7.2.2 Oznaczanie i postępowanie z informacją**

Zasady oznaczania i postępowania z informacją w VS DATA określają Właściciele.

## **A.8 Bezpieczeństwo osobowe**

### **Cel: A.8.2 Przed zatrudnieniem**

#### **Zab: A.8.1.1 Role i odpowiedzialności**

Zasady zatrudniania pracowników VS DATA, w tym role i odpowiedzialności w tym obszarze, określa Procedura PR3 -1 Zarządzanie zasobami ludzkimi.

#### **Zab: A.8.1.2 Sprawdzanie**

Na etapie selekcji i rekrutacji kandydatów prowadzone jest ciągle postępowanie sprawdzające potencjalnego pracownika pod kątem predyspozycji na dane stanowisko pracy, umiejętności i opinii środowiskowej, także pod kątem bezpieczeństwa informacji.

Nabór kandydatów na dane stanowisko pracy odbywa się poprzez zamieszczenie ogłoszenia w lokalnej prasie, oraz na stronie internetowej [www.vsdata.pl](http://www.vsdata.pl). Kandydaci składają aplikacje zgodnie z listą dokumentów zawartych w ogłoszeniu. Kierownictwo zatwierdza kandydata do zatrudnienia.

### **Zab: A.8.1.3 Warunki zatrudnienia**

Przed podpisaniem umowy o pracę kandydat przedstawia zaświadczenie z Krajowego Rejestru Karnego o niekaralności, jeżeli wymaga tego charakter pracy, i składa oświadczenie o zachowaniu w tajemnicy wszelkich informacji, jakie uzyska podczas pełnienia obowiązków służbowych. Kandydat jest zatrudniony na okres próbny. W tym okresie jest oceniany pod kątem adekwatności na dane stanowisko oraz otrzymuje Poświadczenie bezpieczeństwa lub upoważnienie do przetwarzania danych osobowych, jeżeli jest wymagane na stanowisku pracy.

Poświadczenie bezpieczeństwa jest wydawane na czas określony, okres zależy od stopnia poufności informacji, do których poświadczenie ma zastosowanie. Do momentu uzyskania poświadczenia bezpieczeństwa pracownik nie ma dostępu do informacji niejawnych / tajnych / zastrzeżonych. Poświadczenie wydaje Pełnomocnik Informacji Niejawnych. Poświadczenia w 1 egzemplarzu archiwizowane są u Pełnomocnika, 2 egzemplarz otrzymuje pracownik, kopia Poświadczenia bezpieczeństwa potwierdzona za zgodność z oryginałem przekazywana jest do kadr i umieszczana w Aktach osobowych pracownika. Po okresie próbnym pracownik zostaje zatrudniony na czas określony z możliwością dostępu do informacji niejawnych / tajnych / zastrzeżonych (jeżeli wymaga tego stanowisko pracy).

W zakresie obowiązków, uprawnień i odpowiedzialności, który jest integralną częścią umowy o pracę, umieszczone są zapisy dotyczące ochrony danych (osobowych, informacji niejawnych itp.).

Zastosowanie w/w procedur ma miejsce w odniesieniu do każdego pracownika, wyjątkiem jest grupa pracowników gospodarczych (np. sprzątaczką).

### **Cel: A.8.2 Podczas zatrudnienia**

#### **Zab: A.8.2.1 Odpowiedzialność kierownictwa**

Właściciele VS DATA wymagają od pracowników i klientów Spółki oraz pozostałych użytkowników stanowiących strony trzecie, by stosowali środki bezpieczeństwa zgodnie z ustanowioną przez VS DATA Polityką Bezpieczeństwa Informacji i politykami SZBI.

Jedną z form weryfikacji postępowania pracowników VS DATA na zgodność z ustanowioną przez Spółkę Polityką Bezpieczeństwa Informacji i politykami SZBI jest system auditów wewnętrznych oraz przeglądy zarządzania i przeglądy kadrowe, podczas których WŁ przeprowadzają rozmowy oceniające z każdym z pracowników.

Przegląd umów o pracę wraz zakresem obowiązków, uprawnień i odpowiedzialności (zawarte są tam zapisy dotyczące ochrony informacji niejawnych, danych osobowych, danych finansowych itp. – wynikające z przepisów prawa) oraz Stanowiskową kartą pracy (zawiera wymagania stawiane pracownikowi na danym stanowisku pracy) dokonywany jest na bieżąco – przy okazji zmian organizacyjnych, ruchów kadrowych.

#### **Zab: A.8.2.2 Świadomość w zakresie bezpieczeństwa informacji, edukacja i szkolenia.**

Każdy pracownik VS DATA w momencie zatrudnienia jest każdorazowo przeszkolony (instruktaż stanowiskowy) z zakresu ochrony danych osobowych, informacji niejawnych, systemu informatycznego.

Okresowo organizowane są szkolenia na podstawie planu szkoleń (aktualizacja wymagań przepisów prawnych w zakresie ochrony danych osobowych, informacji niejawnych, zamówień publicznych, finansów, aktualizacja wymagań normy ISO 9001 oraz ISO 27001, polityk i procedur ZSZ J i BI).

Na etapie wdrożenia SZBI pracownicy / użytkownicy VS DATA zostali przeszkoleni z zakresu wymagań SZBI oraz polityki i procedur związanych z bezpieczeństwem informacji.

### **Zab: A.8.2.3 Postępowanie dyscyplinarne**

W przypadku, gdy pracownik przekracza swoje uprawnienia lub nie wypełnia zapisów umowy o pracę (zakres obowiązków, uprawnień i odpowiedzialności) oraz nie przestrzega zapisów Polityki Bezpieczeństwa Informacji i polityk SZBI, podlega odpowiedzialności dyscyplinarnej zgodnie Kodeksem Pracy: np. upomnienie i okresowe zablokowanie dostępu – cofnięcie uprawnień, nagana, zwolnienie dyscyplinarne.

Polityka Bezpieczeństwa Informacji oraz poszczególne polityki SZBI zawierają zapis o pociągnięciu do odpowiedzialności dyscyplinarnej w przypadku nie stosowania zapisów z nich wynikających.

## **Cel: A.8.2 Ustanie lub zmiana zatrudnienia**

### **Zab: A.8.3.1 Odpowiedzialności związane z ustaniem zatrudnienia**

Pracownik odchodzący z pracy wypełnia Kartę obiegową oraz składa Oświadczenie o zachowaniu w tajemnicy bezterminowo wszelkich informacji pozyskanych w trakcie wykonywania pracy w VS DATA. Oświadczenie umieszczane jest w Aktach osobowych pracownika.

Przepisy prawa ogólnie obowiązujące ograniczają możliwość wykorzystania danych w dalszej pracy zawodowej pracownika - zakaz zatrudnienia pracownika Spółki przez okres 3 lat w jednostkach konkurencyjnych. Tam gdzie jest to wymagane przepisami prawa pracownik składa w ciągu 30 dni od ustania stosunku pracy deklarację majątkową.

### **Zab: A.8.3.2 Zwrot zasobów**

Pracownik odchodzący z pracy ze Spółki zdaje wszystkie narzędzia przypisane do stanowiska pracy – loginy, hasła, sprzęt komputerowy itp. Przed odejściem pracownik musi uzupełnić Kartę obiegową, która jest zabezpieczeniem zwrotu wszystkich wykorzystywanych przez danego pracownika zasobów.

### **Zab: A.8.3.3 Cofnięcie praw dostępu**

Każdy pracownik odchodzący z pracy z VS DATA na podstawie Karty obiegowej zdaje ST swój login (identyfikator) oraz zasoby sprzętowe przypisane do stanowiska pracy.

ST dokonuje likwidacji konta użytkownika wraz z likwidacją uprawnień dostępu do sieci. Login i hasło użytkownika zostaje zablokowane, tak aby nie można było się nimi posłużyć.

Prawa dostępu do zasobów informacji lub do urządzeń przetwarzania informacji stron zewnętrznych powinny być im odebrane przed zakończeniem kontraktu lub umowy.

Całość postępowania w tym obszarze przebiega zgodnie z Polityką kontroli dostępu do systemu SZBI\_Pol\_04 oraz Polityką postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

## A.9 Bezpieczeństwo fizyczne i środowiskowe

### Cel: A.9.2      **Obszary bezpieczne**

#### **Zab: A.9.1.1    Fizyczna granica obszaru bezpiecznego**

- W VS DATA są wydzielone strefy – pomieszczenia kwalifikowane jako obszary bezpieczne tzw. strefy bezpieczeństwa. Lokalizacja przy ul. Świętojańskiej 55/15, gdzie mieści się siedziba Spółki i podzielona jest na trzy strefy zgodnie ze Schematem pomieszczeń zamieszczony w PR2-1 ISO 9001

Osobami upoważnionymi do przebywania w strefie 2,3 są jedynie osoby upoważnione, zgodnie z opracowanym wykazem.

Granice stref bezpieczeństwa stanowią mury, drzwi wejściowe zabezpieczone zamkami i kartami dostępu.

W strefach bezpieczeństwa znajdują się informacje i urządzenia do przetwarzania informacji wrażliwych lub niejawnych (wrażliwe, do użytku służbowego).

#### **Zab: A.9.1.2    Fizyczne zabezpieczenie wejścia**

Strefy bezpieczeństwa są zabezpieczone przed dostępem osób nieuprawnionych poprzez stosowanie zabezpieczeń fizycznych i proceduralnych typu: hasła i loginy, zamki i karty dostępu, zamykanie na klucz szafy, szafki itp., Polityka kontroli dostępu do systemu, Polityka dostępu do pomieszczeń w strefach bezpieczeństwa, Polityka czystego biurka i czystego pulpitu, procedury postępowania, Zarządzenia Właścicieli VS DATA, wyznaczone godziny i dni pracy - automatyczne wylogowanie z systemu, dostęp do określonych zasobów sieci, upoważnienia, rejestry, audyty, przeglądy, alerty, itp

#### **Zab: A.9.1.3    Zabezpieczenie biur, pomieszczeń i urządzeń**

Zabezpieczenie biur, pomieszczeń i urządzeń w strefach bezpieczeństwa realizowane jest przez stosowanie zabezpieczeń fizycznych i proceduralnych wskazanych w pkt. [Zab:A.9.1.2](#).

W VS DATA funkcjonuje zasada zarządzania kluczami: są pomieszczenia ogólnie dostępne i tzw. strefy bezpieczeństwa (o szczególnym nadzorze), po opuszczeniu pomieszczeń należy zakodować alarm za pomocą karty dostępu, zamknąć pokój na klucz. Klucze zapasowe do pomieszczeń w strefach bezpieczeństwa – przechowywane są w kasetce metalowej.

W zakresie kluczy do szaf, szafek, szuflad w pomieszczeniach biurowych obowiązuje indywidualna polityka zarządzania tymi kluczami z zachowaniem zasady, że ktoś kto nie powinien mieć do nich dostępu nie wie gdzie są przechowywane. Generalnie na biurku/szafce nie powinno być nic – prócz aktualnie wykorzystywanych dokumentów i sprzętu - polityka czystego biurka.

#### **Zab: A.9.1.4    Zabezpieczenie przed zagrożeniami zewnętrznymi i środowiskowymi**

Ochrona fizyczna przed zagrożeniami zewnętrznymi i środowiskowymi jest zaplanowana i wdrożona: w całym budynku są gaśnice, lokalizacja posiada Instrukcję bezpieczeństwa przeciwpożarowego.

### **Zab: A.9.1.5 Praca w obszarach bezpiecznych**

Dostęp do stref bezpieczeństwa mogą mieć jedynie osoby upoważnione, posiadające poświadczenie bezpieczeństwa (jeśli jest taki wymóg!) oraz aktualny login i hasło w zakresie dostępu do zasobów informacyjnych sieci informatycznej VS DATA.

### **Zab: A.9.1.6 Dostęp publiczny, obszary dostaw i załadunku**

Obszar przyjmowania sprzętu (nośników) znajduje się w pomieszczeniu nr 1 (pokój przyjęć), jest izolacja pozostałych pomieszczeń poprzez ich zamykanie.

## **Cel: A.9.2 Zabezpieczenie sprzętu**

### **Zab: A.9.2.1 Rozmieszczenie sprzętu i jego ochrona**

Sprzęt jest tak umiejscowiony, aby zminimalizować dostęp do niego osób niepowołanych. Monitory odwrócone tyłem do drzwi, do klienta, okna; szafki zamykane na klucz przy wyjściu do toalety i do domu; rzeczy chowane przy wyjściu do domu; dokumenty z drukarki sieciowej od razu zabierane, itp.

Urządzenia do przetwarzania szczególnie wrażliwych danych oraz informacji niejawnych są odizolowane, umiejscowione w strefach bezpieczeństwa, gdzie dostęp ograniczony jest do osób upoważnionych.

W miarę możliwości spożywanie posiłków odbywa się z dala od komputerów, W sieci elektrycznej do zasilania komputerów zainstalowane są dwustopniowe zabezpieczenia przeciwprzebiegowe. Sieć zasilająca komputery jest oddzielona od sieci teleinformatycznej.

Całość postępowania w tym obszarze przedstawiona jest w Polityce postępowania ze sprzętem i nośnikami danych SZBI-Pol\_03 oraz Polityce czystego biurka i czystego pulpitu SZBI\_Pol\_05.

### **Zab: A.9.2.2 Urządzenia podtrzymujące**

Sprzęt jest chroniony przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez:

- Zapewnienie odpowiednich warunków atmosferycznych w pomieszczeniu, w którym znajdują się serwer – temperatura, wilgotność.
- Urządzenia podtrzymujące zasilanie UPS przy każdym stanowisku komputerowych.
- Zapewnienie dwustopniowej łączności telekomunikacyjnej: łączność radiowa GSM i kablowa TP S.A. – kilka numerów.

Urządzenia podtrzymujące są omówione w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

### **Zab: A.9.2.3 Bezpieczeństwo okablowania**

Kable zasilające / sieciowe są schowane, tak aby zabezpieczyć je przed uszkodzeniem. Są stosowane oznaczenia kabli, gniazdek oraz jest zachowana rozdzielność kabli sieciowych, zasilających i telekomunikacyjnych.

Kwestia bezpieczeństwa okablowania jest omówiona w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03

#### **Zab: A.9.2.4 Konserwacja sprzętu**

Sprzęt jest na bieżąco konserwowany i przeglądany przez ST, który prowadzi Rejestr konserwacji sprzętu, gdzie wpisywany jest zakres napraw / prac. Całość postępowania w tym obszarze jest zgodna z Polityką postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

#### **Zab: A.9.2.5 Zabezpieczenie sprzętu poza siedzibą**

Generalnie obowiązuje zasada, że sprzęt i nośniki nie są wynoszone poza siedzibę VS DATA. W przypadku osób upoważnionych / uprzywilejowanych obowiązują pewne zasady postępowania w celu zapewnienia bezpieczeństwa informacji. Kwestia zabezpieczenia sprzętu poza siedzibą omówiona została w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

#### **Zab: A.9.2.6 Bezpieczne usuwanie sprzętu lub przekazywanie do ponownego użycia**

W przypadku zmiany właściciela – przekazanie sprzętu dysk jest formatowany, tak aby danych z dysku nie można było odtworzyć i tylko taki sprzęt jest przekazany do nowego właściciela / użytkownika.

Zgłoszenie awarii – zepsuty twardy dysk do ST. Sposób postępowania: jeżeli jest możliwość dane z dysku są zgrywane, uszkodzony dysk przechowywany (deponowany)

Zmiana właściciela – przekazanie sprzętu. Sposób postępowania: dane są kopiowane, dysk jest bezpiecznie czyszczony i formatowany, tak aby dane z dysku nie można było odtworzyć i taki sprzęt jest przekazany do nowego właściciela / użytkownika.

Całość postępowania w tym obszarze omówiona jest w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

#### **Zab: A.9.2.7 Wynoszenie mienia**

Generalnie obowiązuje zasada, że sprzęt i nośniki danych nie są wynoszone poza siedzibę Spółki. W przypadku pozostałego mienia w Spółce obowiązuje bezwzględny zakaz wynoszenia poza siedzibę. Zasady postępowania w przypadku wynoszenia poza siedzibę Spółki np. komputerów przenośnych przedstawione są w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

## **A.10 Zarządzanie komunikacją i eksploatacją**

### **Cel: A.10.2 Procedury i odpowiedzialności w zakresie eksploatacji**

#### **Zab: A.10.1.1 Udokumentowane procedury eksploatacji**

Odpowiedzialności i sposoby postępowania w zakresie korzystania z urządzeń do przetwarzania informacji, oprogramowania oraz zasobów informatycznych sieci zostały określone w niniejszej Księdze, Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03, Polityce zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji SZBI\_Pol\_06, Polityce kontroli dostępu do systemu SZBI\_Pol\_04, Polityce kontroli oprogramowania SZBI\_Pol\_08, Polityce dostępu do pomieszczeń w strefach bezpieczeństwa SZBI\_Pol\_07, aktach prawnych (dane osobowe, informacje niejawne), zakresach obowiązków, uprawnień i odpowiedzialności, rejestrach (np.

rejestr zestawień zbiorczych dla zestawu komputerowego z oświadczeniem/deklaracją użytkownika o przestrzeganiu Polityk SZBI).

### **Zab: A.10.1.2 Zarządzanie zmianą**

Zmiany w urządzeniach do przetwarzania informacji oraz w systemie i nowe oprogramowanie (fizyczna instalacja) są nadzorowane przez ST. Użytkownik ma możliwości wprowadzania zmian w systemie w związku z rodzajem wykonywanej pracy. Przedstawiciel kierownictwa ds. systemu zarządzania jakością i bezpieczeństwa informacji (PJ) prowadzi Rejestr oprogramowania w postaci zbioru Kart Zestawienie zbiorcze dla zestawu (użytkownik, oprogramowanie), w przypadku nowego oprogramowania jest robiony zapis na Karcie. Na Karcie znajduje się kilka punktów mówiących o obowiązkach i uprawnieniach użytkownika w formie oświadczenia (m.in. zakaz instalowania oprogramowania przez użytkownika, obowiązek przestrzegania zapisów Polityk SZBI). Karta jest podpisana przez użytkownika i zarchiwizowana w aktach osobowych pracownika.

W przypadku awarii systemu stosowana jest procedura ponownego uruchamiania i odtwarzania systemu. komputery na bieżąco są reinstalowane / przeinstalowane / czyszczone i zawsze kopia dysku jest robiona. Przy reinstalacji systemu wszystkie dane z komputera są archiwizowane i wgrywane ponownie po zakończonej reinstalacji systemu.

Zagadnienia związane z zarządzaniem zmianą poruszone są w Politykach SZBI: Polityka postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03, Polityka kontroli dostępu do systemu SZBI\_Pol\_04, Polityka zarządzania incydentami i słabościami związanymi z bezpieczeństwem informacji SZBI\_Pol\_06, Polityka dostępu do pomieszczeń w strefach bezpieczeństwa SZBI\_Pol\_07, Polityka kontroli oprogramowania SZBI\_Pol\_08.

### **Zab: A.10.1.3 Podział obowiązków**

Podział obowiązków pracowników VS DATA jest odzwierciedlony w zakresach obowiązków, uprawnień i odpowiedzialności, opisach stanowisk pracy, prawach dostępu (poświadczenia bezpieczeństwa, loginy i hasła), Politykach SZBI, procedurach i instrukcjach oraz Zarządzeniach WŁ VS DATA.

Podział obowiązków zapewnia minimalizację ryzyka przypadkowego lub rozmyślnego nadużycia systemu.

### **Zab: A.10.1.4 Oddzielanie urządzeń będących w eksploatacji od przeznaczonych do prac rozwojowych**

VS DATA nie prowadzi prac rozwojowych. Testowanie aplikacji aktualizacji odbywa się na maszynach wirtualnych - wyłączenie

## **Cel: A.10.2 Zarządzanie dostarczaniem usług przez strony trzecie**

### **Zab: A.10.2.1 Dostarczanie usług**

Dostarczanie usług przez strony trzecie odbywa się zgodnie z zawartą umową oraz z zachowaniem bezpieczeństwa informacji przetwarzanej przez VS DATA. Wszystkie umowy cywilno-prawne zawierane przez VS DATA powinny zawierać klauzulę bezpieczeństwa.

### **Zab: A.10.2.2 Monitorowanie i przegląd usług dostarczanych przez strony trzecie**

Usługi, umowy z wykonawcami, raporty i zapisy dostarczone przez strony trzecie są monitorowane i poddawane przeglądom. Przeprowadzane są audyty usług dostarczanych przez strony trzecie. Jest ranking dostawców, prowadzona jest okresowa ocena dostawców zgodnie z wymaganiami normy ISO 9001:2000.

### **Zab: A.10.2.3 Zarządzanie zmianami w usługach świadczonych przez strony trzecie**

W przypadku zmian w świadczeniu usług, będą dokonane odpowiednie ustalenia z Wykonawcą i zapisy (umowy, aneksy do umów, itp.). Jeżeli waga i charakter zmian będzie istotna z punktu widzenia bezpieczeństwa informacji, zostanie przeprowadzony przegląd polityk SZBI i stosowanych zabezpieczeń w celu ulepszenia istniejących polityk, procedur i zabezpieczeń.

## **Cel: A.10.2 Planowanie i akceptacja systemu**

### **Zab: A.10.3.1 Zarządzanie pojemnością**

Zarządzanie pojemnością systemu informatycznego nadzorowany jest przez ST. Na bieżąco monitorowana jest pojemność sieci komputerowej (serwery, stacje robocze). Przy zakupie nowego sprzętu pojemność zawsze uwzględnia przyszłe potrzeby. Technologia i standard wykorzystywanego sprzętu znaczenie przekracza obecne potrzeby.

### **Zab: A.10.3.2 Odbiór systemu**

Kryteria odbioru systemu dla nowych systemów i upgrade'ów, określone są w umowach ze stronami zewnętrznymi. W przypadku wdrażania nowych systemów zawsze w umowie z firmą zewnętrzną jest zapis o przeszkoleniu osób korzystających oraz o bezpieczeństwie (klauzula bezpieczeństwa) podczas integracji z obecnie działającym systemem. Po upgrade'ach jest sprawdzanie poprawności działania programu.

Kryteria odbioru systemu zgodnie z zawartymi umowami, po aktualizacji lub modernizacji poprawność działania programu testowana jest na maszynach wirtualnych.

## **Cel: A.10.2 Zabezpieczenie przeciwko złośliwemu i mobilnemu oprogramowaniu**

### **Zab: A.10.4.1 Zabezpieczenie przeciwko złośliwemu oprogramowaniu**

W VS DATA są wdrożone zabezpieczenia przeciwko złośliwemu oprogramowaniu – oprogramowanie antywirusowe, firewall software'owy, program antywirusowy - okresowa automatyczna aktualizacja i automatyczne skanowanie systemów operacyjnych oraz właściwe procedury postępowania i uświadamiania użytkowników systemu. Procedury te przedstawione są w Polityce kontroli oprogramowania SZBI\_PoI\_08.

### **Zab: A.10.4.2 Zabezpieczenie przeciwko mobilnemu oprogramowaniu**

Wyłączenie. Oprogramowanie mobilne nie jest dopuszczane do wewnętrznych systemów informatycznych.

## **Cel: A.10.2 Kopie zapasowe**

### **Zab: A.10.5.1 Kopie zapasowe informacji**

Zasady, tryb oraz zakres tworzenia kopii zapasowych informacji przedstawione są w Polityce tworzenia kopii zapasowych i archiwizacji informacji SZBI\_Pol\_02.

## **Cel: A.10.2 Zarządzanie bezpieczeństwem sieci**

### **Zab: A.10.6.1 Zabezpieczenia sieci**

W celu zachowania bezpieczeństwa danych przetwarzanych w sieci VS DATA stosowanych jest szereg zabezpieczeń wskazanych w niniejszej Księdze, Politykach SZBI, Procedurach ZSZJ i BI oraz Deklaracji stosowania zabezpieczeń (SZBI\_Pol\_01\_SzacowanieRyzyka).

### **Zab: A.10.6.2 Bezpieczeństwo usług sieciowych**

Sieć jest obsługiwana i zarządzana przez ST, w przypadku dostępu do sieci przez strony zewnętrzne wymagane jest zawarcie w umowie warunków dostępu oraz klauzuli bezpieczeństwa.

## **Cel: A.10.2 Postępowanie z nośnikami**

### **Zab: A.10.7.1 Zarządzanie wymiennymi nośnikami**

Procedura zarządzania wymiennymi nośnikami zawarta jest w dokumencie Polityki postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03. Stosowanie osobistych nośników możliwe jest tylko w obrębie organizacji i w godzinach pracy.

### **Zab: A.10.7.2 Niszczanie nośników**

W przypadku zmiany właściciela nośnika lub sprzętu każda informacja zawarta na dysku jest backupowana przez ST i przechowywana w organizacji (kopia przechowywana jest przez ST).

Całość postępowania w tym obszarze omówiona jest w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

### **Zab: A.10.7.3 Procedury postępowania z nośnikami**

Procedura postępowania z nośnikami danych zawarta jest w dokumencie Polityki postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

### **Zab: A.10.7.4 Bezpieczeństwo dokumentacji systemu**

Dokumentacja Sytemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz dokumentacja systemów informatycznych jest przechowywana u Pełnomocnika ds. Zintegrowanego Systemu Zrządzania Jakością i Bezpieczeństwem Informacji (ZSZ J i BI). Dokumentacja SZBI w oryginalnym wydaniu papierowym jest przechowywana u PJ.

Nadzór nad dokumentacją SZBI jest prowadzony zgodnie z Procedura PR5-1 Nadzór nad dokumentami i zapisami.

## **Cel: A.10.2      Wymiana informacji**

### **Zab: A.10.8.1    Polityki i procedury w zakresie wymiany informacji**

W celu ochrony informacji przetwarzanej przez VS DATA przed nieuprawnionym ujawnieniem lub nadużyciem wprowadzone zostały procedury postępowania z informacją obejmujące posługiwanie się, przetwarzanie, przesyłanie / wymianę, oznaczanie i przechowywanie informacji zgodnie z jej klasyfikacją.

Procedury postępowania z informacją opisane są w niniejszej Księdze, aktach prawnych (dane osobowe, informacje niejawne) oraz Politykach SZBI.

Procedury dotyczące wymiany informacji zawarte są w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03, Polityce kontroli dostępu do systemu SZBI\_Pol\_04, Polityce dostępu do pomieszczeń w strefach bezpieczeństwa SZBI\_Pol\_07, . Procedury wymiany informacji wrażliwych (dane osobowe) i niejawnych wynikają z przepisów prawnych - Ustawa o ochronie danych osobowych, Ustawa o ochronie informacji niejawnych. W VS DATA funkcjonuje elektroniczny system obiegu dokumentów, który wymusza na pracownikach VS DATA stosowanie zasad proceduralnych w zakresie postępowania z informacją.

Ochrona wymiany informacji będzie realizowana poprzez zastosowanie wszystkich rodzajów urządzeń komunikacyjnych, formalne polityki, procedury i zabezpieczenia wymiany

### **Zab: A.10.8.2    Umowy w zakresie wymiany**

W przypadku wymiany informacji między VS DATA a stronami zewnętrznymi, zostaną zawarte umowy odnośnie wymiany informacji, oraz zostaną ustalone i wdrożone zabezpieczenia zgodnie z zapisami procedur wymiany informacji. Ilość i rodzaj zabezpieczeń zależy od wagi i wrażliwości informacji.

### **Zab: A.10.8.3    Nośniki fizyczne podczas transportu**

W celu zabezpieczenia fizycznych nośników danych podczas transportu powinny być wdrożone zabezpieczenia chroniące przed nieuprawnionym dostępem, nadużyciem lub uszkodzeniem tych nośników. Zasady postępowania z nośnikami danych, także podczas transportu, zawarte są w Polityce postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

### **Zab: A.10.8.4    Elektroniczne wiadomości**

Informacje przekazywane przez pracowników VS DATA za pośrednictwem poczty elektronicznej są chronione przed nieuprawnionym dostępem i modyfikacją przez stosowanie zabezpieczeń typu: dostęp do konta pocztowego ma użytkownik po zalogowaniu się w sieci, Jest dozwolone wykorzystanie Gadu - Gadu do komunikacji.

Elektroniczny obieg dokumentów umożliwia automatyczną archiwizację maili i załączonych plików w systemie obiegu informacji (Informatyczny system zarządzania informacją i procesami pracy). System ten umożliwia elektroniczną komunikację wewnętrzną z opcją dołączania załączników.

### **Zab: A.10.8.5    Systemy informacji biznesowej**

Informacje dotyczące wzajemnych połączeń systemów informacji biznesowej są chronione poprzez stosowanie zabezpieczeń typu: .

- Informacje w formie papierowej przekazywane są do sekretariatu, który następnie przekazuje je do poszczególnych komórek VS DATA. Informacje w formie papierowej przesyłane są do klientów firmy drogą pocztową, bądź poprzez kuriera.

Sposób postępowania i zabezpieczenia w tym obszarze zawarte są w niniejszej Księdze oraz Politykach SZBI: Polityka szacowania ryzyka SZBI\_Pol\_01, Polityka postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03, Polityka kontroli dostępu do systemu SZBI\_Pol\_04.

## **Cel: A.10.2 Bezpieczeństwo handlu elektronicznego**

### **Zab: A.10.9.1 Handel elektroniczny**

Wyłączenie. VS DATA nie prowadzi działalności w obszarze handlu elektronicznego.

### **Zab: A.10.9.2 Transakcje on-line**

Wyłączenie. VS DATA nie prowadzi działalności w obszarze handlu elektronicznego.

### **Zab: A.10.9.3 Publicznie dostępna informacja**

Publicznie dostępne informacje znajdują się na stronie internetowej [www.vsdata.pl](http://www.vsdata.pl).

## **Cel: A.10.2 Monitorowanie**

### **Zab: A.10.10.1 Logi dla potrzeb auditu**

Nie stosuje się oprogramowania zarządzającego planowaniem i prowadzeniem auditu. Nie tworzone są logi w systemie. -WYŁĄCZENIE

### **Zab: A.10.10.2 Monitorowanie użycia systemu**

Jest prowadzone monitorowanie użycia systemu z uwzględnieniem ryzyka. Dostęp do systemu informatycznego VS DATA jest ograniczony do dni i godzin pracy VS DATA (praca poza godzinami wymaga zgłoszenia) oraz do osób uprawnionych (zdefiniowanych jako użytkownik sieci, z ważnym/aktualnym loginem i hasłem). Dostęp do Internetu jest monitorowany, dostępność do zasobów sieci jest ograniczona do osób uprawnionych. Monitorowanie użycia systemu jest prowadzone z uwzględnieniem ryzyka

### **Zab: A.10.10.3 Zabezpieczenie informacji z logów**

Informacje z logów są zabezpieczone przed nieuprawnionym dostępem i modyfikacją - użytkownik nie ma możliwości zmiany logów – blokada dokonana przez ST, logi przechowywane są na serwerze.

### **Zab: A.10.10.4 Logi administratora i użytkownika**

Logi administratora – jest włączony system logowania czynności. Logi użytkowników komputerów, gdzie są przetwarzane dane osobowe są archiwizowane. Ustawa o ochronie

danych osobowych nakłada obowiązek zachowania logów przetwarzania tych danych. Logi użytkownika tworzone na każdym innym komputerze są nadpisywane.

#### **Zab: A.10.10.5 Logi błędów**

Logi błędów to logi z alertów są archiwizowane na serwerze. W przypadku wystąpienia jakiegoś błędu w sieci informatycznej Administrator sieci IT jest automatycznie informowany o tym przez alerty.

#### **Zab: A.10.10.6 Synchronizacja zegarów**

Czas jest automatycznie synchronizowany z serwerem domeny Windows.

## **A.11 Kontrola dostępu**

### **Cel: A.11.2 Potrzeby biznesowe związane z dostępem do systemu**

#### **Zab: A.11.1.1 Polityka kontroli dostępu**

Dostęp do informacji jest ograniczony do osób upoważnionych / uprawnionych oraz jest nadzorowany. Procedury postępowania w tym obszarze zostały zdefiniowane i udokumentowane. Dostęp jest ograniczony zgodnie z zakresem określonym w Polityce kontroli dostępu do systemu SZBI\_Pol\_04, Polityce czystego biurka i czystego pulpitu SZBI\_Pol\_05, Polityce zarządzania incydentami i słabościami związanymi z bezpieczeństwem informacji SZBI\_Pol\_06, Polityce dostępu do pomieszczeń w strefach bezpieczeństwa SZBI\_Pol\_07, Polityce kontroli oprogramowania SZBI\_Pol\_08.

### **Cel: A.11.2 Zarządzanie dostępem użytkowników**

#### **Zab: A.11.2.1 Rejestrowanie użytkowników**

Zasady i tryb rejestrowania / wyrejestrowania użytkowników systemu informatycznego VS DATA określone są w Polityce kontroli dostępu do systemu SZBI\_Pol\_04.

#### **Zab: A.11.2.2 Zarządzanie przywilejami**

Przyznawanie i używanie przywilejów w zakresie dostępu do informacji jest ograniczone przepisami prawa - Ustawa o ochronie danych osobowych, Ustawa o ochronie informacji niejawnych. O przyznawaniu przywilejów decydują WŁ..

#### **Zab: A.11.2.3 Zarządzanie hasłami użytkowników**

Zasady przydzielania i administrowania hasłami zawarte są w Polityce kontroli dostępu do systemu SZBI\_Pol\_04 oraz Polityce czystego biurka i czystego pulpitu SZBI\_Pol\_05.

Każdy użytkownik komputera posiada swoje hasło dostępu i login (identyfikator), które musi wprowadzać za każdym razem po uruchomieniu, wygaszeniu, wylogowaniu komputera. Hasła są w formie zaszyfrowanej, jest blokowanie wyświetlania i zapamiętywania

hasła, oraz składają się z ciągu znaków alfanumerycznych odpowiedniej długości. Hasła w systemie są przechowywane w innym miejscu niż dane systemu aplikacji.

#### **Zab: A.11.2.4 Przegląd praw dostępu użytkowników**

Przeglądy praw dostępu użytkowników do zasobów sieci informatycznej łącznie z czasowymi przywilejami przeprowadzane są w trakcie auditów wewnętrznych i w ramach prowadzonej kontroli przez WŁ.

### **Cel: A.11.2 Zakres odpowiedzialności użytkowników**

#### **Zab: A.11.3.1 Użycie haseł**

Definiowanie i użycie haseł powinno przebiegać zgodnie z ustalonymi procedurami w tym obszarze, zawartymi w Polityce kontroli dostępu do systemu SZBI\_Pol\_04 oraz Polityce czystego biurka i czystego pulpitu SZBI\_Pol\_05.

Hasło użytkownika systemu powinno być skonstruowane w taki sposób aby utrudnić jego identyfikację. Hasła użytkowników systemu są regularnie zmieniane – system wymusza zmianę hasła po upływie określonego czasu. Hasła nie mogą się powtarzać w określonych cyklach czasowych – system nie przyjmie starego hasła oraz haseł używanych do 3 cykli wstecz. Hasła, loginów nie zapisuje się w miejscach ogólnie dostępnych (np. na karteczkach przyklejanych do monitorów, tablicach, kalendarzach). Każdy użytkownik ma obowiązek chronić hasło i login oraz zapewnić brak dostępu do tych informacji przez osoby nieupoważnione.

#### **Zab: A.11.3.2 Pozostawianie sprzętu użytkownika bez opieki**

Obowiązuje generalna zasada, że uruchomionego sprzętu ze stanem aktywności w sieci użytkownik nie zostawia bez opieki. System automatycznie wylogowuje nieaktywnego użytkownika z sieci po upływie określonego czasu. Ponowne zalogowanie wymaga wprowadzenia identyfikatora i hasła.

Na użytkowniku sprzętu spoczywa odpowiedzialność za wszystkie aktywa, również informacyjne, związane z tym sprzętem. Obowiązkiem użytkownika jest stosowanie określonych procedur i zabezpieczeń adekwatnie do sytuacji oraz wagi i wrażliwości informacji, np. wygaszasz ekranu z hasłem, wylogowanie się z systemu, nie pozostawianie przenośnego sprzętu komputerowego oraz nośników danych w miejscach publicznych bez nadzoru itp. .

#### **Zab: A.11.3.3 Polityka czystego biurka i ekranu**

W VS DATA obowiązuje Polityka czystego biurka i czystego pulpitu SZBI\_Pol\_05 w odniesieniu do dokumentów papierowych, przenośnych nośników danych i danych elektronicznych zawierających informacje wrażliwe lub niejawne.

Obowiązuje generalna zasada, że na biurku pracownika VS DATA znajdują się jedynie dokumenty w danej chwili wykorzystywane, oraz, że na pulpitach komputerów nie prowadzi się zapisywania / tymczasowego zapisywania plików.

## **Cel: A.11.2      Kontrola dostępu do sieci**

### **Zab: A.11.4.1    Polityka korzystania z usług sieciowych**

Zasady korzystania z usług sieciowych zawarte są w Polityce kontroli dostępu do systemu SZBI\_Pol\_04, zgodnie z którą użytkownicy mają zapewniony bezpośredni dostęp tylko do tych usług / zasobów informacyjnych w sieci, do których mają aktualne uprawnienia.

### **Zab: A.11.4.2    Uwierzytelnianie użytkowników przy połączeniach zewnętrznych**

Brak dostępu z zewnątrz do sieci wewnętrznej z zewnątrz.

### **Zab: A.11.4.3    Identyfikacja urządzeń w sieciach**

Identyfikacja urządzeń w sieci jest poprzez adres fizyczny karty sieciowej (MAC Adres) urządzenia.

### **Zab: A.11.4.4    Ochrona zdalnych portów diagnostycznych i konfiguracyjnych**

Cały ruch internetowy, za wyjątkiem portów, które służą do przeglądania stron WWW, obsługi poczty elektronicznej, FTP (transfer plików), zablokowany jest poprzez Firewall

### **Zab: A.11.4.5    Rozdzielanie sieci**

Wspólna sieć dla wszystkich użytkowników (dostęp dla nieautoryzowanych użytkowników jest wyłączony). Brak rozdzielności sieci.

### **Zab: A.11.4.6    Kontrola połączeń sieciowych**

Kwestia kontroli połączeń sieciowych zawarta jest w Polityce kontroli dostępu do systemu SZBI\_Pol\_04 oraz w niniejszej Księdze.

Ruchy w obrębie sieci oraz z sieci na zewnątrz i odwrotnie kontrolowane są przez Firewalle (zapory, bramka).

Wszystkie komputery w sieci lokalnej VS DATA mają dostęp do poczty e-mail. Serwer poczty elektronicznej jest obsługiwany przez zewnętrzną firmę na podstawie umowy. WŁ mają możliwość administracji kontami użytkowników w ograniczonym zakresie: założyć, usunąć, zmiana hasła, pojemność skrzynki, filtry antyspamowe. Jest rejestr posiadaczy kont e-mail wraz z ich adresami na serwerze pocztowym. WŁ mają dostęp do serwera zabezpieczony loginem i hasłem.

### **Zab: A.11.4.7    Kontrola routingu w sieciach**

Routing (narzucanie z góry określonej trasy / drogi połączeń jaką będą przesyłane informacje) ma zastosowanie w przypadku wymiany informacji z sieci wewnętrznej do sieci Internet.

## **Cel: A.11.2      Kontrola dostępu do systemów operacyjnych**

### **Zab: A.11.5.1    Bezpieczne procedury rejestrowania terminalu w systemie**

Każde urządzenie w sieci jest rejestrowane i identyfikowane za pomocą fizycznego adresu karty sieciowej – MAC Adres. Tylko urządzenie, którego MAC Adres jest zdefiniowany w systemie przez Administratora IT może zalogować się w sieci informatycznej VS DATA

### **Zab: A.11.5.2 Identyfikacja i uwierzytelnianie użytkowników**

Każdy użytkownik sieci informatycznej ma nadany swój login i hasło dostępu. Hasła są przesyłane w sieci w formie zaszyfrowanej. Blokowanie wyświetlania i zapamiętywania haseł. Hasła w systemie są przechowywane w innym miejscu niż dane systemu aplikacji. System wymusza zmianę hasła po upływie określonego czasu, hasła nie mogą się powtarzać do 3 cykli wstecz (system zapamiętuje hasła).

### **Zab: A.11.5.3 System zarządzania hasłami**

Polityka zarządzania hasłami zawarta jest w Polityce kontroli dostępu do systemu SZBI\_Pol\_04 oraz Polityce czystego biurka i czystego pulpitu SZBI\_Pol\_05.

ST, przy pierwszym logowaniu się do systemu użytkownik generuje swoje własne hasło - system wymusza zmianę hasła, itp. Zabezpieczenia fizyczne: system wymusza zmianę hasła po upływie określonego czasu, hasła nie mogą się powtarzać do 3 cykli wstecz - system zapamiętuje hasła, wygaszacz ekranu z hasłem, itp.

### **Zab: A.11.5.4 Użycie systemowych programów narzędziowych**

Dostęp do systemowych programów narzędziowych jest kontrolowany i nadzorowany przez ST.

W VS DATA są 2 poziomy dostępu do systemu: z poziomu użytkownika i administratora. Tylko administrator ma możliwość dostępu do systemowych programów narzędziowych.

### **Zab: A.11.5.5 Wyłączanie terminalu po określonym czasie nieaktywności**

W przypadku dłuższej nieaktywności w sieci komputery automatycznie wylogowują się z sieci (zamykanie używanych aplikacji) i uruchamiany jest wygaszacz ekranu. Ponowne uruchomienie / powrót do systemu wymaga wprowadzenia loginu i hasła użytkownika.

### **Zab: A.11.5.6 Ograniczenie czasu trwania połączenia**

Czasu trwania dostępu do połączeń ograniczony został do pór połączeń normalnych godzin biurowych.

## **Cel: A.11.2 Kontrola dostępu do informacji i aplikacji**

### **Zab: A.11.6.1 Ograniczenie dostępu do informacji**

Dostęp do informacji i funkcji systemowych aplikacji jest ograniczony zgodnie z Polityką kontroli dostępu do systemu SZBI\_Pol\_04, Polityką czystego biurka i czystego pulpitu SZBI\_Pol\_05, Polityką dostępu do pomieszczeń w strefach bezpieczeństwa SZBI\_Pol\_07.

Są wyizolowane miejsca, z ograniczonym dostępem, z zabezpieczeniami (system alarmowy, system kontroli dostępu, zamki, drzwi, szafy i szafki zamykane na klucz), gdzie przechowywane są informacje i aplikacje wrażliwe, niejawnie – tzw. strefy bezpieczeństwa. Dostęp do stref bezpieczeństwa ograniczony jest do osób upoważnionych.

### **Zab: A.11.6.2 Izolowanie systemów wrażliwych**

Systemy wrażliwe (serwer / komputery przetwarzające informacje wrażliwe lub niejawne) są izolowane – tworzenie stref bezpieczeństwa.

Dostęp do pomieszczeń w strefach bezpieczeństwa jest chroniony przez system kontroli dostępu. Ograniczony dostęp do osób upoważnionych - określone osoby mają prawo wejścia do tych pomieszczeń, inne osoby mogą wejść tylko w obecności i pod nadzorem osób upoważnionych. Zabezpieczenia typu: system alarmowy, system kontroli dostępu, zamki, drzwi, szafy i szafki zamykane na klucz.

### **Cel: A.11.2 Komputery przenośne i praca na odległość**

#### **Zab: A.11.7.1 Przenośne komputery i urządzenia komunikacyjne**

W zakresie zasad bezpieczeństwa dotyczących przenośnych urządzeń komputerowych typu: notebook, palmtop oraz komunikacyjnych - telefony komórkowe obowiązuje Polityka postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03.

Zabezpieczenia fizyczne i proceduralne: login i hasło, wygaszacz ekranu z hasłem, kopie zapasowe, ochrona antywirusowa, zasady przenoszenia i obchodzenia się ze sprzętem poza lokalizacją VS DATA itp.

#### **Zab: A.11.7.2 Praca na odległość**

W przypadku pracy na odległość w Spółce stosowane są Zabezpieczenia proceduralne - hasło wejścia do systemu, ograniczenie lokalizacji fizycznych (host, ip) obsługiwanych przez system. Kompetencje i odpowiedzialności - zakresy obowiązków, procedury, instrukcje, polityki SZBI, Księga SZBI, zarządzenia i in.

## **A.12 Pozyskanie, rozwój i utrzymanie systemu**

### **Cel: A.12.2 Wymagania bezpieczeństwa systemów IT**

#### **Zab: A.12.1.1 Analiza i opis wymagań bezpieczeństwa**

Wymagania biznesowe VS DATA dotyczące nowych systemów informacyjnych i informatycznych, lub dotyczące rozszerzenia / rozwoju / ulepszenia dla istniejących systemów, uwzględniają wymagania dotyczące bezpieczeństwa informacji. Wymagania te zawarte są w umowach ze stronami zewnętrznymi (klauzule bezpieczeństwa), planach rozwoju Spółki, Politykach SZBI: Polityka kontroli dostępu do systemu SZBI\_Pol\_04, Polityka dostępu do pomieszczeń w strefach bezpieczeństwa SZBI\_Pol\_07, Planie postępowania z ryzykiem i Procedurach ZSZ J i BI: Wymagania dotyczące bezpieczeństwa informacji przetwarzanej przez VS DATA są okresowo przeglądane i oceniane z uwzględnieniem aktualnych wyników szacowania ryzyka i stosowanych zabezpieczeń.

### **Cel: A.12.2 Prawidłowe przetwarzanie w aplikacjach**

#### **Zab: A.12.2.1 Walidacja danych wejściowych**

Dane wejściowe są uwierzytelniane poprzez systemy ochrony antywirusowej, kontroli dostępu (firewall) oraz uwierzytelnianie użytkownika (login i hasło).

#### **Zab: A.12.2.2 Kontrola wewnętrznego przetwarzania**

Kontrola wewnętrznego przetwarzania odbywa się zgodnie z Polityką kontroli dostępu do systemu SZBI\_Pol\_04. Zastosowane są zabezpieczenia tj. loginy, hasła. Dostęp

ograniczony jest do osób upoważnionych. W przypadku wystąpienia awarii systemu do przywrócenia stanu sprzed awarii wykorzystywana jest najbardziej aktualna kopia bezpieczeństwa danych.

#### **Zab: A.12.2.3 Uwierzytelnianie wiadomości (integralność)**

Dane / informacje wpisywane są do systemu informatycznego VS DATA przez uprawnione osoby, które logują się do systemu za pomocą identyfikatora (login) i hasła. Zapewniona jest integralność danych w systemie poprzez dostęp do systemu i modyfikację danych tylko przez osoby upoważnione.

#### **Zab: A.12.2.4 Walidacja danych wyjściowych**

Dane wyjściowe są uwierzytelniane przez walidację całego procesu przetwarzania informacji / danych.

### **Cel: A.12.2 Zabezpieczenia kryptograficzne**

#### **Zab: A.12.3.1 Polityka używania zabezpieczeń kryptograficznych**

Wyłączenie. Brak zabezpieczeń kryptograficznych w VS DATA S.C.

#### **Zab: A.12.3.2 Zarządzanie kluczami**

Wyłączenie. Brak zabezpieczeń kryptograficznych w VS DATA.

### **Cel: A.12.2 Bezpieczeństwo plików systemowych**

#### **Zab: A.12.4.1 Kontrola eksploatowanego oprogramowania**

Oprogramowanie eksploatowane w VS DATA jest kontrolowane i nadzorowane przez ST. Obowiązuje w tym obszarze Polityka kontroli dostępu do systemu SZBI\_Pol\_04 i Polityka kontroli oprogramowania SZBI\_Pol\_08.

Instalacja oprogramowania na komputerach dokonywana jest wyłącznie przez ST (tworzenie obrazu dysku po instalacji/reinstalacji oprogramowania systemowego). Obowiązuje zakaz samodzielnego instalowania jakiegokolwiek oprogramowania przez pracowników – użytkownik podpisuje oświadczenie w tym zakresie (Zestawienie zbiorcze dla zestawu). Rejestr oprogramowania zainstalowanego na danym stanowisku pracy w postaci zbioru Kart Zestawienie zbiorcze dla zestawu komputerowego . Przeprowadzane są okresowe przeglądy stanowisk pracy pod kątem oprogramowania i sprzętu (szczególnie komputery, z których wpłynął alert z programu antywirusowego lub alert błędów).

#### **Zab: A.12.4.2 Ochrona systemowych danych testowych**

W przypadku kiedy zachodzi potrzeba generowania i przetwarzania systemowych danych testowych, dane te są dobrane w sposób zapewniający bezpieczeństwo i integralność źródłowych danych systemowych. Dane wybierane są z systemu w sposób losowy, tak aby nie stanowiły źródła informacji, w takiej formie udostępniane do testów, a następnie trwale niszczone. Uprawnienia i odpowiedzialność w tym zakresie ma tylko ST.

### **Zab: A.12.4.3 Kontrola dostępu do bibliotek programów źródłowych**

Użytkownicy nie mają dostępu do systemowych katalogów aplikacji / oprogramowania na serwerze / komputerze. Dostęp do bibliotek programów źródłowych ma tylko ST.

System Windows sam w sobie ma zabezpieczenia, które blokują dostęp do bibliotek programów źródłowych.

## **Cel: A.12.2 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej**

### **Zab: A.12.5.1 Procedury kontroli zmian**

W przypadku wprowadzania zmian, modyfikowany obszar zostanie poddany analizie ryzyka przed i po wdrożeniu tych zmian w celu możliwości kontroli tych zmian i ich wpływu na bezpieczeństwo informacji.

### **Zab: A.12.5.2 Przegląd techniczny aplikacji po zmianach w systemie operacyjnym**

Po wprowadzeniu zmian systemy aplikacji są poddawane testom. W przypadku zwiększenia liczby użytkowników w sieci: przed włączeniem nowego użytkownika do sieci oprogramowanie systemowe jest sprawdzane na zgodność z ustalonym wzorcem instalacji systemu operacyjnego oraz innymi wymaganiami typu: uprawnienia użytkownika, po włączeniu użytkownika do sieci sprawdzana jest poprawność ustawień i komunikacji z serwerami sieci w zakresie dostępności do zasobów.

Żaden użytkownik nie może sam zainstalować oprogramowania – tylko ST instaluje oprogramowanie, po zainstalowaniu nowego oprogramowania jest przeprowadzany przegląd techniczny aplikacji.

### **Zab: A.12.5.3 Ograniczenie dotyczące zmian w pakietach oprogramowania**

Zmiany w pakietach oprogramowania są ściśle kontrolowane – tylko ST dokonać takich zmian. Na komputerach jest włączona blokada zmian w pakietach oprogramowania przez użytkownika. Polityka kontroli oprogramowania

### **Zab: A.12.5.4 Wyciek informacji**

Zarządzanie informacją w VS DATA jest prowadzone pod kątem zapobiegania wyciekowi informacji. Wszystkie działania i zastosowane rozwiązania techniczne i technologiczne mają na celu zapewnienie bezpieczeństwa, integralności i dostępności informacji.

### **Zab: A.12.5.5 Prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej**

WYŁĄCZENIE. Nie występują prace rozwojowe nad oprogramowaniem wykorzystywanym przez VS DATA powierzone stronom zewnętrznym. Oprogramowanie wykorzystywane przez VS DATA jest upgradowane z aktualizacji dostępnych na rynku.

## **Cel: A.12.2 Zarządzanie techniczną podatnością na zagrożenia**

### **Zab: A.12.6.1 Kontrolowanie technicznej podatności na zagrożenia**

Techniczna podatność systemu informacyjnego i informatycznego VS DATA na zagrożenia związane z bezpieczeństwem informacji jest zidentyfikowana (Raport z szacowania ryzyka) oraz jest stale kontrolowana i aktualizowana.

## **A.13 Zarządzanie incydentami związanymi z bezpieczeństwem informacji**

### **Cel: A.13.2 Zgłaszanie zdarzeń i słabości związanych z bezpieczeństwem informacji**

#### **Zab: A.13.1.1 Raportowanie zdarzeń związanych z bezpieczeństwem informacji**

Polityka zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji SZBI\_Pol-06 określa sposób postępowania i odpowiedzialności w zakresie raportowania zdarzeń związanych z bezpieczeństwem informacji.

Zgodnie z tą Polityką każdy kto zauważy zdarzenie, sytuację skutkującą lub mogącą skutkować naruszeniem bezpieczeństwa informacji ma obowiązek to zgłosić Właścicielom.

#### **Zab: A.13.1.2 Raportowanie słabości związanych z bezpieczeństwem**

Raportowanie słabości związanych z bezpieczeństwem informacji przebiega analogicznie jak raportowanie incydentów. Postępowanie w tym obszarze jest zgodne z Polityką zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji SZBI\_Pol-06.

### **Cel: A.13.2 Zarządzanie incydentami i ulepszeniami związanymi z bezpieczeństwem informacji**

#### **Zab: A.13.2.1 Odpowiedzialności i procedury**

Procedury i odpowiedzialności dotyczące zarządzania incydentami i ulepszeniami związanymi z bezpieczeństwem informacji zawarte są w Polityce zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji SZBI\_Pol-06.

#### **Zab: A.13.2.2 Nauka z incydentów związanych z bezpieczeństwem informacji**

W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji lub zidentyfikowania słabości systemu, wdrażane są działania korygujące lub zapobiegawcze w zależności od sytuacji, zgodnie z Polityką zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji SZBI\_Pol-06 oraz Procedurą działania korygujące i zapobiegawcze PR4-4. Każde zdarzenie / sytuacja mogąca skutkować naruszeniem bezpieczeństwa informacji lub której następstwem jest naruszenie bezpieczeństwa informacji jest analizowana w celu dojścia do przyczyny wystąpienia i wdrożenia odpowiednich środków zaradczych.

Rejestr incydentów SZBI\_Pol\_06 (incydent, przyczyna, koszt usunięcia, wdrożone działania korygujące) jest regularnie przeglądany przez WŁ w celu nauki z incydentów i analizy skuteczności SZBI.

### **Zab: A.13.2.3 Zbieranie dowodów**

Polityka zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji SZBI\_Pol\_06 określa sposób postępowania i odpowiedzialności w obszarze zarządzania incydentami. Alerty o błędach są przechowywane u ST. W przypadku wystąpienia incydentu są zbierane dowody i sporządzane zapisy.

W przypadku wystąpienia incydentu są zbierane dowody i sporządzane zapisy zgodnie z Procedurą działania korygujące i zapobiegawcze PR4-4. Jeżeli zgłoszony incydent może powodować wszczęcie postępowania karnego, dyscyplinarnego lub cywilnego w stosunku do osoby lub organizacji WŁ mają obowiązek zebrać i zabezpieczyć oraz przedstawić dowody na żądanie odpowiednich władz.

## **A.14 Zarządzanie ciągłością działania**

### **Cel: A.14.2 Aspekty zarządzania ciągłością działania związane z bezpieczeństwem informacji**

#### **Zab: A.14.1.1 Włączanie bezpieczeństwa informacji w proces zarządzania ciągłością działania**

Bezpieczeństwo informacji jest integralną częścią procesu zarządzania ciągłością działania VS DATA.

W planach / strategiach rozwoju VS DATA uwzględnianych jest szereg inwestycji / rozwiązań w kierunku podniesienia lub zapewnienia bezpieczeństwa informacji, np. wdrożenie i utrzymanie SZBI.

Bezpieczeństwo informacji oraz urządzeń do przetwarzania informacji jest uwzględnione w takich dokumentach jak:

- Instrukcja bezpieczeństwa pożarowego dla budynków VS DATA – klauzula „jawny”,
- Polityka ciągłości działania SZBI\_Pol\_09.

Dokumenty te zawierają m.in. wytyczne co do sposobu postępowania z nośnikami danych (dokumenty papierowe, dane na nośnikach elektronicznych) oraz sprzętem IT w przypadku wybuchu wojny, pożaru lub zaistnienia innej sytuacji kryzysowej.

#### **Zab: A.14.1.2 Ciągłość działania i analiza ryzyka**

Zdarzenia / sytuacje, które mogą spowodować przerwy w działalności VS DATA zostały określone oraz uwzględnione w analizie ryzyka – Raport z szacowania ryzyka. Został oszacowany wpływ i ewentualne konsekwencje takich zdarzeń w odniesieniu do bezpieczeństwa informacji oraz zabezpieczenia i środki zaradcze.

#### **Zab: A.14.1.3 Tworzenie i wdrażanie planów ciągłości działania uwzględniających bezpieczeństwo informacji**

VS DATA ma plany ciągłości działania w różnych sytuacjach kryzysowych (wojna, pożar, powódź itp.):

- Instrukcja bezpieczeństwa pożarowego dla budynków VS DATA – klauzula „jawny”; określa sposób postępowania i odpowiedzialności w przypadku wybuchu pożaru, sposób ewakuacji ludzi i mienia ze szczególnym uwzględnieniem zasobów informacyjnych na nośnikach danych (dokumenty papierowe, dyskietki, płyty CD, dyski wymienne, pamięć zewnętrzna itp.) i sprzętu do przetwarzania informacji (sprzęt IT);
- Archiwizacja danych wrażliwych i niejawnych umożliwiająca odtworzenie systemu pozwalającego na ciągłość działania.

Zasady tworzenia / opracowania i wdrażania w/w planów zawarte są w Polityce ciągłości działania SZBI\_Pol\_09.

#### **Zab: A.14.1.4 Struktura planowania ciągłości działania**

Struktura planowania ciągłości działania przedstawiona jest w Polityce ciągłości działania SZBI\_Pol\_09.

#### **Zab: A.14.1.5 Testowanie, utrzymywanie i ponowna ocena planów ciągłości działania**

Plany ciągłości działania są sprawdzane / testowane pod kątem adekwatności i aktualności. Sposób postępowania i odpowiedzialności w zakresie testowania, utrzymywania i oceny / aktualizacji planów ciągłości działania zawarte są w Polityce ciągłości działania SZBI\_Pol\_09.

## **A.15 Zgodność**

### **Cel: A.15.2 Zgodność z przepisami prawa**

#### **Zab: A.15.1.1 Identyfikacja odpowiednich przepisów prawnych**

Prawo jest identyfikowane przez WŁ oraz wszystkich pracowników VS DATA.

#### **Zab: A.15.1.2 Prawo do własności intelektualnej**

VS DATA nie tworzy własności intelektualnej. Własność intelektualna wykorzystywana przez Spółkę dotyczy oprogramowania i jego aktualizacji – wykupione licencje i aktualizacje. Wszystkie programy wykorzystywane przez Spółkę posiadają ważne licencje. Nadzór nad oprogramowaniem sprawowany jest przez ST.

W przypadku tworzenia dóbr intelektualnych na zlecenie VS DATA w umowie z wykonawcą jest zapis o przekazaniu praw autorskich do dzieła.

#### **Zab: A.15.1.3 Zabezpieczanie zapisów organizacji**

Zapisy są tworzone, autoryzowane, przechowywane, zabezpieczane i niszczone zgodnie z Procedurą nadzoru nad dokumentami i zapisami PR5-1, Polityką tworzenia kopii zapasowych i archiwizacji informacji SZBI\_Pol\_02, Polityką postępowania ze sprzętem i nośnikami danych SZBI\_Pol\_03, Polityką kontroli dostępu do systemu SZBI\_Pol\_04, Polityką czystego biurka i czystego pulpitu SZBI\_Pol\_05.

#### **Zab: A.15.1.4 Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych**

Przetwarzanie danych osobowych oraz dostęp do tych danych jest uregulowane w odpowiednich przepisach prawnych (Ustawa o ochronie danych osobowych) oraz w procedurach i politykach obowiązujących w VS DATA.

Stosowane są odpowiednie zabezpieczenia zgodne z wymaganiami zawartymi w w/w regulacjach: zabezpieczenia fizyczne i proceduralne typu szafy i szafki zamykane na klucz, pomieszczenia zamykane na klucz, dostęp chroniony jest loginem i hasłem oraz ograniczony jest do osób uprawnionych, określone procedury postępowania wynikające z przepisów prawa.

#### **Zab: A.15.1.5 Zapobieganie nadużywaniu urządzeń przetwarzających informacje**

Dostęp do urządzeń przetwarzających informacje jest ograniczony i kontrolowany – dostęp jest możliwy tylko przez osoby uprawnione.

Urządzenia przetwarzające informacje mogą być wykorzystywane w ściśle określony sposób i do określonych zadań zgodnych z ich przeznaczeniem.

Wdrożone są procedury zapobiegające nadużywaniu tych urządzeń, np. użytkownicy komputerów / notebook'ów nie mają prawa i możliwości instalować na nich oprogramowania.

#### **Zab: A.15.1.6 Regulacje dotyczące zabezpieczeń kryptograficznych**

Wyłączenie. Brak zabezpieczeń kryptograficznych.

### **Cel: A.15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna**

#### **Zab: A.15.2.1 Zgodność z politykami bezpieczeństwa i standardami**

Wszystkie działania związane z przetwarzaniem informacji są zgodne z politykami / procedurami bezpieczeństwa i normami bezpieczeństwa.

#### **Zab: A.15.2.2 Sprawdzanie zgodności technicznej**

Skuteczność zabezpieczeń jest okresowo przeglądana pod kątem jej zgodności technicznej w odniesieniu do zmian technologicznych podczas auditów wewnętrznych i zewnętrznych, kontroli oprogramowania i sprzętu, szkoleń, instruktazu, przeglądu systemu itd.

### **Cel: A.15.2 Rozważania dotyczące audytu systemu**

#### **Zab: A.15.3.1 Zabezpieczenia audytu systemów IT**

Audity systemu informatycznego VS DATA przeprowadzane są w zaplanowanych odstępach czasu zgodnie z harmonogramem auditów. Harmonogram auditu ustalany jest z odpowiednim wyprzedzeniem z kierownikami komórek organizacyjnych, których dotyczą, tak aby zminimalizować zakłócenia w ciągłości pracy.

## Zab: A.15.3.2 Ochrona narzędzi audytu systemów IT

Wyłączenie. VS DATA nie korzysta z oprogramowania auditującego. Audyty przeprowadzane są poprzez bezpośrednią fizyczną kontrolę stanowiska pracy.

## ZAPISY

- Zapisy z bazy danych dbvsd.

## DOKUMENTY ZWIĄZANE

- Norma 27001:2005
- Procedury ZSZJ i BI:
  - PR5-1 Nadzór nad dokumentacją i zapisami ZSZJ i BI
  - PR4-1 Przegląd zarządzania Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji wykonywany przez VS DATA
  - PR3-1 Zarządzania zasobami ludzkimi VS DATA
  - PR4-2 Audyty wewnętrzne ZSZ J i BI
  - PR4-4 Działania korygujące i zapobiegawcze
- Polityki SZBI:
  - SZBI\_Pol\_01 Polityka szacowania ryzyka
  - SZBI\_Pol\_02 Polityka tworzenia kopii zapasowych i archiwizacji informacji
  - SZBI\_Pol\_03 Polityka postępowania ze sprzętem i nośnikami danych
  - SZBI\_Pol\_04 Polityka kontroli dostępu do systemu
  - SZBI\_Pol\_05 Polityka czystego biurka i czystego pulpitu
  - SZBI\_Pol\_06 Polityka zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji
  - SZBI\_Pol\_07 Polityka dostępu do pomieszczeń w strefach bezpieczeństwa
  - SZBI\_Pol\_08 Polityka kontroli oprogramowania
  - SZBI\_Pol\_09 Polityka ciągłości działania
- Deklaracja stosowania zabezpieczeń SZBI\_Pol\_01\_DeklaracjaStosowania
- Plan postępowania z ryzykiem 01\_SZBI\_Pol\_01\_PlanPostepowaniaZRyzykiem
- Raport z szacowania ryzyka 01\_SZBI\_Pol\_01\_SzacowanieRyzyka
- Ustawa o ochronie informacji niejawnych,
- Wewnętrzne akty regulujące, w tym: Zarządzenia WŁ VS DATA

## HISTORIA ZMIAN DOKUMENTU

DATA EDYCJI	WERSJA	TREŚĆ ZMIANY
2008.02.20	1.0	Wersja Pierwotna
2008.06.09	1.1	Zmiana strony tytułowej – przewidziano miejsce na podpis