1. Program należytej staranności w zakresie bezpieczeństwa informacji dla podmiotów trzecich jest dokumentem opisującym zasady ochrony informacji w celu spełnienia wymagań cyberbezpieczeństwa i wymagań prawnych.

2. Program należytej staranności w zakresie bezpieczeństwa informacji dla podmiotów trzecich jest poddawany przeglądom w zaplanowanych odstępach czasu, nie rzadziej niż raz w roku lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że jest właściwa, adekwatna i skuteczna. Przegląd obejmuje szacowanie możliwości doskonalenia, z uwzględnieniem zmian środowiska organizacyjnego, wymagań prawnych lub środowiska technicznego.

§ 2

Definicje

1. W Polityce bezpieczeństwa informacji przyjmuje się następujące definicje stosowanych pojęć:

a) **aktywa** - wszystko, co ma wartość dla organizacji
b) **analiza ryzyka** - systematyczne wykorzystywanie informacji do zidentyfikowania źródeł ryzyka i jego oszacowania
c) **analiza zagrożeń** - badanie działań i zdarzeń, które mogą szkodliwie wpływać na system przetwarzania danych,
d) **audyt bezpieczeństwa** - niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamania bezpieczeństwa oraz zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach,
e) **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów, jak użytkownicy, procesy, systemy i informacja
f) **badanie zgodności** - przeprowadzenie testów i dokonanie ocen bezpieczeństwa w celu ustalenia zgodności ze specyfikacją i z wymaganiami systemu bezpieczeństwa,
g) **bezpieczeństwo** - stan lub ochrona przed niekontrolowanymi stratami lub skutkami, kombinacja usług zapewniających poufność, integralność i dostępność,
h) **bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność
i) **bezpieczeństwo systemu informatycznego** - wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu informatycznego,
j) **ciągłość działania** - utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak pożar lub trzęsienie ziemi, lub zdarzeniami wywołanymi umyślnie, np. sabotażem,
k) **dokumentacja** - pisemna lub zarejestrowana w innej formie informacja o przedmiocie oceny, wymagana do jego oceny,

l) **dostępność** - oznacza zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne
m) **incydent związany z bezpieczeństwem informacji** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji
n) **integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności aktywów
o) **ocena ryzyka** - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
p) **podatność** - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie,
q) **polityka bezpieczeństwa** - zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu,
r) **poufność** - właściwość wskazująca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom
s) **rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
t) **ryzyko** - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów
u) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji
v) **szacowanie ryzyka** - szacowanie zagrożeń, ich wpływu, podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia,
w) **zabezpieczenie** - praktyka, procedura lub mechanizm redukujący ryzyko,
x) **zagrożenie** - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji,
y) **zdarzenie związane z bezpieczeństwem informacji** - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

§ 3

Opis zdarzeń naruszających bezpieczeństwo informacji

1. Podział zagrożeń bezpieczeństwa informacji:
1) **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona - nie dochodzi do naruszenia poufności danych;
2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu - może nastąpić naruszenie poufności danych;

3) **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- nieuprawniony przekaz danych,
- pogorszenie jakości sprzętu i oprogramowania,
- bezpośrednie zagrożenie materialnych składników systemu.
- przechwycenie sygnałów na skutek zjawiska interferencji
- szpiegostwo zdalne
- podsłuch
- kradzież nośników lub dokumentów lub urządzenia
- odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników
- ujawnienie
- manipulowanie urządzeniem
- sfałszowanie oprogramowania

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane to:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) nastąpiła niedopuszczalna manipulacja danymi w systemie;
9) ujawniono osobom nieupoważnionym dane lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.;

12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, tj. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych w celach prywatnych, itp. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pendrive, czy przenośnych dyskach HD w formie niezabezpieczonej itp.

§ 4

Inwentaryzacja i zabezpieczenie sprzętu komputerowego

1. Strona trzecia wykonuje i prowadzi na bieżąco inwentaryzację sprzętu wykorzystywanego do przetwarzania informacji oraz oprogramowania.

2. Inwentaryzacja zasobów informatycznych polega na ustaleniu w stopniu wyczerpującym i kompletnym:
   a) jakie urządzenia są wykorzystywane do przetwarzania danych,
   b) jakie oprogramowanie jest wykorzystywane do przetwarzania danych,
   c) kategorii informacji przetwarzanych na konkretnych, odnotowanych co do tożsamości urządzeniach,
   d) miejscu ich przechowywania,
   e) osobach, które mogą mieć dostęp do oprogramowania

3. Celem zabezpieczenia sprzętu jest zapobieżenie utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji. Zaleca się umieszczenie i ochronę sprzętu w taki sposób, aby zminimalizować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.

4. W celu ochrony sprzętu zaleca się rozważenie ulokowania sprzętu w taki sposób, aby zminimalizować niepotrzebny dostęp do obszarów pracy, takiego ulokowania środków przetwarzania wrażliwych informacji, aby podczas ich użycia minimalizować ryzyko podglądu przez nieuprawnione osoby, urządzenia przechowujące informacje powinny być zabezpieczone w sposób uniemożliwiający nieuprawniony dostęp, wprowadzenie zabezpieczeń minimalizujących ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, np. kradzieżą, pożarem, dymem, zalaniem (lub awarią zaopatrzenia w wodę), kurzem, wibracjami, środkami chemicznymi, interferencjami linii zasilających, promieniowaniem elektromagnetycznym i wandalizmem.

§ 5

Konserwacja sprzętu komputerowego

1. W celu zapewnienia ciągłej dostępności i integralności sprzętu komputerowego strona trzecia nadzoruje prawidłową konserwację, zgodnie z zaleceniami dostawcy, w zakresie częstotliwości i zakresu, naprawianie lub serwisowanie sprzętu tylko przez autoryzowany personel, rejestrowanie wszystkich podejrzewanych lub rzeczywistych awarii oraz prewencyjnych i korygujących czynności konserwacyjnych.

2. Strona trzecia nadzoruje wdrożenie odpowiednich zabezpieczeń na czas czynności konserwacyjnych, z uwzględnieniem działań przeprowadzanych na miejscu lub poza siedzibą organizacji; jeśli zachodzi taka potrzeba, konieczne jest usuwanie poufnych informacji ze sprzętu lub nadanie personelowi utrzymującemu odpowiednich uprawnień, zapewnienie zgodności z wszystkimi wymaganiami dotyczącymi konserwacji.

3. Strona trzecia kontroluje urządzenie przed jego ponownym uruchomieniem, po przeprowadzeniu jego konserwacji, w celu zapewnienia, że sprzęt nie został zmanipulowany i nie realizuje szkodliwych funkcji.

§ 6

Bezpieczeństwo sprzętu i aktywów poza siedzibą - urządzenia mobilne i telepraca

1. Należy zabezpieczyć aktywa wynoszone poza siedzibę organizacji przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.

2. Zaleca się, aby korzystanie ze środków przechowywania i przetwarzania informacji poza siedzibą organizacji było autoryzowane. Ma to zastosowanie zarówno do urządzeń, jakimi dysponuje organizacja, jak i prywatnych, używanych w imieniu organizacji.

3. W kwestii ochrony sprzętu znajdującego się poza siedzibą, nie należy pozostawiać w miejscach publicznych bez nadzoru urządzeń lub nośników wynoszonych poza siedzibę organizacji, przestrzegać instrukcji producenta dotyczących ochrony sprzętu, np. ochrony przed wystawieniem na działanie silnego pola elektromagnetycznego.

4. Należy stosować odpowiednie zabezpieczenia określone w czasie procesu szacowania ryzyka, niezbędne podczas pracy poza siedzibą, np. pracując zdalnie, w tymczasowych lokalizacjach, takie jak zamykane szafki, polityka czystego biurka, zabezpieczenia dostępu do komputerów oraz bezpieczne połączenie z biurem.

5. Zaleca się, aby wybierając właściwe zabezpieczenia uwzględnić fakt, że ryzyka np. uszkodzeń, kradzieży lub podsłuchu, mogą znacząco różnić się w zależności od miejsca. W przypadku wystąpienia ryzyka kradzieży, utraty sprzętu na którym przechowywane są istotne dane np. dane wrażliwe, informacje na sprzęcie powinny być przechowywane w formie zaszyfrowanej.

6. Zaleca się zachowanie ostrożności podczas korzystania z urządzeń mobilnych w miejscach publicznych, salach konferencyjnych i innych niezabezpieczonych obszarach.

7. Zaleca się stosowanie środków ochrony, aby uniknąć nieautoryzowanego dostępu do tych urządzeń lub ujawnienia informacji przechowywanych i przetwarzanych przez te urządzenia, na przykład poprzez zastosowanie technik kryptograficznych i wymuszanie wykorzystania poufnych informacji uwierzytelniających.

8. Zaleca się również fizycznie zabezpieczenie urządzeń mobilnych przed kradzieżą, zwłaszcza pozostawionych na przykład w samochodach oraz innych środkach transportu, pokojach hotelowych, centrach konferencyjnych i miejscach spotkań.

§ 7

Zasada czystego biurka i czystego ekranu

1. Należy przestrzegać zasady czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz zasady czystego ekranu dla środków przetwarzania informacji.

2. Należy przestrzegać następujące rozwiązania organizacyjne:
a) przechowywania pod zamknięciem informacji umieszczonych na nośnikach elektronicznych lub w postaci dokumentów papierowych, szczególnie jeśli pomieszczenie biurowe jest opuszczane;
b) zamykania sesji lub blokowanie komputerów pozostawionych bez opieki za pomocą mechanizmu blokowania ekranu i klawiatury zabezpieczanego hasłem, lub z użyciem innego podobnego mechanizmu uwierzytelnienia użytkownika; ochrony komputerów i terminali mechanicznym zamkiem, hasłem lub za pomocą innego zabezpieczenia jeśli nie są używane;
c) niezwłoczne usuwanie z drukarek wydruków zawierających wrażliwe informacje.

§ 8

Bezpieczeństwo systemów informatycznych i danych. Kopie zapasowe

1. W systemie informatycznym służącym do przetwarzania danych Strona trzecia wprowadza mechanizm kontroli dostępu do tych danych, a w przypadku, kiedy dostęp do danych przetwarzanych w systemie informatycznym posiadają, co najmniej dwie osoby, musi być zapewnione, aby:
   a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
   b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

2. Strona trzecia zapewnia, aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie.

3. System informatyczny służący do przetwarzania danych musi być zabezpieczony, w szczególności przed:
a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

4. Podczas tworzenia kopii zapasowych zaleca się:
a) utworzenie dokładnego i kompletnego spisu kopii zapasowych
b) aby zakres (np. pełny lub przyrostowy) i częstotliwość kopii zapasowych odzwierciedlały wymagania związane z bezpieczeństwem informacji oraz krytyczność informacji dla ciągłości działalności organizacji;
c) przechowywanie kopii zapasowych w innej lokalizacji, w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęła ośrodek podstawowy
d) odpowiednie fizyczne zabezpieczenie kopii zapasowych oraz zabezpieczenie ich przed wpływem środowiska
e) testowanie nośników kopii zapasowych, aby można było na nich polegać w przypadku awaryjnego odtwarzania; zaleca się łączenie powyższego z testami procedur odtwarzania i sprawdzaniem wymaganego czasu odtworzenia. Badanie zdolności do przywracania danych z kopii zapasowej zaleca się wykonać na dedykowanych testowych nośnikach, a nie poprzez nadpisanie oryginalnego nośnika, gdyby utworzenie kopii zapasowej lub przywrócenie danych nie powiodło się i spowodowało nieodwracalne uszkodzenie lub utratę danych;
f) w sytuacjach, gdy ważna jest poufność, szyfrowanie kopii zapasowych.
5. Zaleca się regularne testowanie planów kopii zapasowych pojedynczych systemów i usług, aby spełniały wymagania planów ciągłości działania. W przypadku systemów i usług krytycznych zaleca się, aby plany te obejmowały wszystkie informacje systemowe, aplikacje oraz dane niezbędne do odtworzenia całego systemu na wypadek awarii.

6. Dane przetwarzane w systemie informatycznym muszą być zabezpieczone przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe muszą być:
   a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem,
   b) modyfikacją, uszkodzeniem lub zniszczeniem;
   c) przechowywane jeżeli to możliwe w formie zaszyfrowanej;
   d) usuwane niezwłocznie po ustaniu ich użyteczności.

7. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji - muszą zostać pozbawione wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - muszą zostać pozbawione wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

c) naprawy — muszą zostać pozbawione wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

8. Systemy informatyczne służące do przetwarzania danych muszą być chronione przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. W przypadku zastosowania zabezpieczeń, muszą one obejmować:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

9. Urządzenia i nośniki zawierające dane, przekazywane poza obszar, w którym dane są przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność tych danych m.in. poprzez przechowywanie ich na tych urządzeniach i nośnikach w formie zaszyfrowanej.

§ 9

Zasady korzystania z Internetu

1. Użytkownik Strony trzeciej zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą strony trzeciej i tylko w uzasadnionych przypadkach.

2. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

3. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

4. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

5. Cyberprzestępstwo to wszelkiego rodzaju działalność przestępcza, która odbywa się za pomocą komputerów lub innych tego typu urządzeń elektronicznych Często

miejscem działania jest również Internet. W związku z tym, że przestępcy mają różne metody działania i korzystają z różnego rodzaju narzędzi, wyróżnić można kilka rodzajów cyberprzestępczości:

a) Phishing to rodzaj oszustwa, którego celem jest wyłudzenie ważnych danych, takich jak na przykład numer karty kredytowej lub dane do logowania (np. do bankowości internetowej) itp. W tym celu cyberprzestępcy podszywają się pod określoną osobę lub instytucję darzoną zaufaniem (np. bank) w wiadomości mailowej, czy poprzez fałszywą stronę internetową.
b) Malware to różnego rodzaju złośliwe oprogramowanie, które może zainfekować komputer. Jego celem jest kradzież danych, zniszczenie plików, czy zablokowanie dostępu do urządzenia. Do tego typu oprogramowania możemy zaliczyć wirusy, robaki, trojany, spyware (oprogramowanie szpiegujące), randomware (blokujące dostęp do określonych zasobów lub systemu komputerowego) itd.
c) Hacking to włamania, poprzez łamanie zabezpieczeń, umożliwiające zdalny, nielegalny dostęp do czyjegoś komputera.
d) Cyberstalking czyli nękanie drugiej osoby przez Internet, poprzez wysyłanie niechcianych wiadomości w mediach społecznościowych, komunikatorach, pocztą elektroniczną.

6. W celu zwiększenia bezpieczeństwa w sieci przedstawiam kilka podstawowych porad, które należy przestrzegać przy korzystaniu z internetu:
   a) zakaz otwierania maili od podejrzanych nadawców. Cyberprzestępcy mogą zainfekować komputer swojej ofiary nawet na skutek samego wyświetlenia przez nią grafik dołączonych do wiadomości mailowej. Warto zatem jak najszybciej usuwać maile od nieznanych i wzbudzających podejrzenie nadawców. Najczęściej będą to wiadomości przesłane z zagranicznej domeny, a ich treść napisana w niedbały sposób z licznymi błędami gramatycznymi Tematyka jest zazwyczaj typowa dla SPAMu, np. powiadomienie o wygranej w konkursie Pod żadnym pozorem nie należy klikać w linki, ani otwierać załączników znajdujących się w takich mailach.
   b) zakaz klikania w reklamy pojawiające się na pulpicie czy w przeglądarce. Do infekcji wirusem, trojanem , oprogramowaniem szpiegującym i innymi szkodliwymi programami może także dojść na skutek kliknięcia w pojawiającą się reklamę. Dlatego warto ignorować tego typu wyskakujące okna i jak najszybciej przeskanować system programem antywirusowym.
   c) tworzenie trudnych do odgadnięcia haseł. Chcąc zadbać o bezpieczeństwo w sieci, należy w jak największym stopniu utrudnić cyberprzestępcom proces rozszyfrowywania haseł np. do systemu bankowości elektronicznej, poczty, routera czy sieci WiFi. Przede wszystkim warto pamiętać, aby nie używać tych samych loginów i haseł w różnych miejscach sieci. Wyjątkowo łatwe do odgadnięcia są hasła w formie daty urodzenia, imienia czy innych krótkich słów Znacznie więcej czasu zajmie hakerowi rozszyfrowanie hasła składającego się z wielu znaków liczb, małych i wielkich liter oraz symboli specjalnych W prosty sposób można je utworzyć, korzystając z darmowych generatorów online.
   d) regularne aktualizacje oprogramowania. Bezpieczeństwo w internecie w ogromnym stopniu zależy od tego, jak często użytkownik aktualizuje system operacyjny, oprogramowanie antywirusowe, a także wszystkie zainstalowane aplikacje Dzięki aktualizacjom możliwe jest bieżące usuwanie luk w

zabezpieczeniach, które mogłyby cyberprzestępcom posłużyć do przeprowadzenia ataku Jeżeli nie jesteś w stanie pamiętać o przeprowadzania aktualizacji w ręczny sposób, warto wtedy aktywować opcję ich automatycznego wgrywania.

e) korzystanie z zapory sieciowej. Zapora sieciowa, to system chroniący komputer znajdujący się w sieci LAN przed nieuprawnionym dostępem z zewnątrz. Zapora monitoruje ruch sieciowy oraz filtruje niebezpieczne połączenia przychodzące i wychodzące Stanowi więc barierę przed różnego typu zagrożeniami internetowymi.

f) wylogowywanie się z serwisów internetowych. Po zakończeniu korzystania z serwisu wymagającego logowania się należy niezwłocznie skorzystać z opcji wylogowania. Dzięki wylogowaniu się zmniejszamy ryzyko, że poufne dane zostaną przejęte przez osobę trzecią.

g) podawanie poufnych danych jedynie na stronach z certyfikatem SSL. Jeżeli podajemy w internecie swoje dane np. rejestrujemy się, wypełniamy formularze elektroniczne czy kupujemy w sklepie online upewniamy się wcześniej, czy dany serwis został zabezpieczony za pomocą protokołu https Sprawdzamy to, klikając w symbol kłódki, znajdujący się obok adresu strony w przeglądarce Jeżeli serwis posiada certyfikat SSL, wtedy otrzymamy komunikat „Połączenie jest bezpieczne".

h) pobieranie plików i programów jedynie z zaufanych źródeł. Jednym z najczęstszych powodów infekcji komputera szkodliwym oprogramowaniem jest pobieranie plików z nielegalnie działających stron Ściągamy pliki jedynie z zaufanych i legalnych źródeł, których wiarygodności jesteśmy pewni.

i) sprawdzenie, czy razem z programem nie instalujemy dodatkowych narzędzi. Często się zdarza, że podczas instalowania legalnego i przydatnego programu można w pakiecie zainstalować szkodliwe narzędzia firm trzecich, które okazują się być złośliwym oprogramowaniem. Dlatego należy dokładnie czytać wyświetlane przez kreator instalacji komunikaty i nie godzić się na wgrywanie dodatkowych komponentów

j) ochrona dostępu do komputera. Nie należy pozostawiać bez nadzoru niezabezpieczonych komputerów. Panującą zasadą jest aby blokować komputery (które powinny być chronione hasłem przy logowaniu) przez pracowników w przypadku oddalania się od biurka.

§ 10

Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania danych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).

3. W przypadku zabezpieczenia plików hasłem, obowiązują minimum znaki: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu. Zaleca się, aby użytkownik podczas przesyłania danych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

5. Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych lub zaszyfrowanie przez kryptowirusy.

6. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.

7. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

8. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

9. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej, tajemnicy przedsiębiorstwa i prawa autorskiego. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

10. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, strona trzecia może wprowadzić kontrolę służbowej poczty elektronicznej pracownika.

11. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

§ 11

Zabezpieczenie przed szkodliwym oprogramowaniem

1. Strona trzecia nadzoruje ochronę przed szkodliwym oprogramowaniem na oprogramowaniu wykrywającym i naprawiającym, na świadomości użytkowników w zakresie bezpieczeństwa informacji oraz właściwych mechanizmach kontroli dostępu oraz zarządzania zmianami. Zaleca się następujące rekomendacje:
   a) zabrania się korzystania z nieautoryzowanego oprogramowania;
   b) wdrożenie zabezpieczeń wykrywających lub zapobiegających użyciu nieautoryzowanego oprogramowania (np. białe listy aplikacji);
   c) wdrożenie zabezpieczeń wykrywających lub zapobiegających użyciu znanych szkodliwych stron webowych lub podejrzewanych o to (np. czarne listy);
   d) ustanowienie ochrony przed ryzykami związanymi z otrzymywaniem plików lub oprogramowania z sieci zewnętrznych albo za pośrednictwem innych mediów, określającej jakie środki ochrony należy wdrożyć;
   e) redukowanie podatności, które mogą być wykorzystane przez szkodliwe oprogramowanie, np. poprzez zarządzanie podatnościami technicznymi;
   f) przeprowadzanie regularnych przeglądów oprogramowania i danych zawartych w systemach obsługujących krytyczne procesy biznesowe; zaleca się przeprowadzenie formalnego dochodzenia w przypadku stwierdzenia obecności niezatwierdzonych plików lub nieautoryzowanych poprawek;
   g) zainstalowanie i regularne uaktualnianie oprogramowania do wykrywania oraz usuwania szkodliwego oprogramowania poprzez skanowanie komputerów i nośników informacji, jako zabezpieczenie prewencyjne lub na bieżąco; zaleca się, aby przeprowadzane skanowania obejmowały:
      - skanowanie wszystkich plików odbieranych poprzez sieci lub na innych nośnikach pamięci pod kątem obecności szkodliwego oprogramowania;
      - skanowanie załączników poczty elektronicznej oraz ściąganych danych pod kątem obecności szkodliwego oprogramowania; zaleca się, aby skanowanie prowadzone było w różnych miejscach, np. na serwerach poczty elektronicznej, stacjach roboczych oraz podczas łączenia się z siecią organizacji;
      - sprawdzanie stron internetowych pod kątem obecności szkodliwego oprogramowania;
   h) stosowanie planów ciągłości działania w celu odtwarzania po ataku szkodliwego oprogramowania, zawierających wszystkie niezbędne dane oraz zestawy procedur związane z wykonywaniem kopii zapasowych oprogramowania i ich odtwarzaniem;
   i) wdrożenie regularnego zbierania informacji, takiego jak subskrypcja list mailowych lub sprawdzanie stron webowych, udostępniających informacje dotyczące szkodliwego oprogramowaniem.

§ 12

Bezpieczne korzystanie z urządzeń mobilnych – służbowych telefonów komórkowych

1. Podczas korzystania z urządzeń mobilnych – służbowych telefonów komórkowych, które mogą także stanowić bogate źródło informacji, w tym dane osobowe: zawierają

listy kontaktów, zdjęcia, filmy, historię lokalizacji, dane medyczne i finansowe – należy przestrzegać następujących zasad bezpieczeństwa:

a) ochrona urządzenia przed niepowołanym dostępem: należy wymyślić i ustawić trudne do odgadnięcia hasło lub skorzystać z możliwości jakie daje czytnik odcisku palca. Pomoże to dodatkowo chronić dane w przypadku kradzieży lub utraty urządzenia.
b) świadomy wybór aplikacji: nie należy instalować aplikacji spoza oficjalnego sklepu, ani takich, które wyglądają podejrzanie. Zwracać uwagę na komunikaty, w których jesteśmy proszeni o przyznanie uprawnień. Przed pobraniem aplikacji należy dowiedzieć się więcej zarówno na jej temat, jak i jej producenta. Uważać na linki znajdujące się w otrzymanych wiadomościach e-mail lub SMS-ach, ponieważ mogą służyć do wprowadzenia w błąd i zainstalowania aplikacji pochodzących od innego producenta lub z nieznanego źródła.
c) nie należy używać bezprzewodowych sieci publicznych w celu logowania się do ważnych serwisów, takich jak: bankowość internetowa, konto pocztowe, czy serwisy społecznościowe. Korzystanie z tych usług będzie bezpieczniejsze, jeśli użyjemy o modemu komórkowego lub połączenia VPN.
d) urządzenia muszą mieć zawsze aktualne oprogramowanie operacyjne, należy zadbać o aktualizacje: podobnie jak komputery, również urządzenia mobilne bywają podatne na zagrożenia. Aktualizowanie na bieżąco systemu, przeglądarki internetowej, pakietu antywirusowego i innych wykorzystywanych aplikacji pomoże ochronić przed atakami i szkodliwym oprogramowaniem.
e) zachować porządek: niektóre aplikacje wykorzystujemy jedynie tymczasowo. Odinstalować te, z których już nie korzystamy. Poprawi to bezpieczeństwo urządzenia.
f) zainstalowanie aplikacji bezpieczeństwa do urządzeń mobilnych, pomoże to w ocenie wszystkich aplikacji znajdujących się w urządzeniu, jak również instalowanych w późniejszym czasie, sygnalizując w razie potrzeby obecność szkodliwego oprogramowania

§ 13

1. Każda Strona trzecia przetwarzająca dane, których administratorem jest BARTEX-BARTOL Sp. z o.o. zapoznaje się z treścią Programu należytej staranności w zakresie bezpieczeństwa informacji dla podmiotów trzecich oraz zobowiązuje się do bezwzględnego stosowania postanowień w niej zawartych.

	stanowisko	imię i nazwisko	data	podpis
Opracował	Menager ds. ESG	Zbigniew Czerwiński	13.03.2025	
zatwierdził	Zarząd	Grzegorz Bartol	13.03.2025	BARTEX Bartol sp. z o.o. V-ce prezes zarządu Grzegorz Bartol