Wytyczne dla bezpieczeństwa informacji

Informacje o dokumencie	
tytuł	IS1-4 IA Wytyczne dotyczące bezpieczeństwa informacji
Skrót/odniesienie do dokumentu:	IS1-4
Utworzono:	09.11.2016
Ostatnia edycja:	14 sierpnia 2024 r
Ilość stron:	7
Poziom poufności:	publiczny
Numer wersji:	2
Stan przetwarzania:	Wydany
Wymaga wydania:	Tak
Wydany dnia:	14.08.2024
Wydany przez: Zarządzanie / ISB	Zatwierdzenie poprzez możliwe do sprawdzenia wydanie ważnej wersji głównej na stronie intranetowej działu IS przez ISB i dyrektora generalnego
Rozporządzenie wchodzi w życie z dniem:	09.01.2024
Właściciel dokumentu:	ISB
Zakres:	Cała grupa IDEAL Automotive Group na całym świecie (IA)

Spis treści

Kierownictwo niniejszym przyjmuje w ramach swojej strategii następujące wytyczne dotyczące bezpieczeństwa informacji:

1. Znaczenie przetwarzania informacji

Przetwarzanie informacji odgrywa kluczową rolę w naszej działalności biznesowej. Wszystkie kluczowe funkcje i zadania strategiczne i operacyjne są w znacznym stopniu wspierane przez technologie informacyjno-komunikacyjne (ICT). Awarie systemów ICT muszą być możliwe do zrekompensowania w krótkim okresie. Nasz biznes nie może upaść nawet w niektórych obszarach. Ponieważ nasza podstawowa kompetencja polega na wspólnym opracowywaniu innowacyjnych produktów we współpracy z klientami i dostawcami, ochrona tych informacji przed nieuprawnionym dostępem i nieautoryzowanymi zmianami ma ogromne znaczenie.

2. Cele nadrzędne

Zapewniona jest dostępność naszych danych i naszych systemów ICT we wszystkich obszarach zależnych od technologii i obszarów komercyjnych, tak aby można było tolerować oczekiwane przestoje. Awarie i nieprawidłowości w systemach danych i teleinformatycznych są dopuszczalne jedynie w ograniczonym zakresie i tylko w wyjątkowych przypadkach (integralność). Wymogi dotyczące poufności mają normalny poziom zorientowany na zgodność z prawem. Informacje, które ze względu na wewnętrzną klauzulę tajności lub wymagania umowne naszych klientów są zaklasyfikowane jako poufne lub tajne i muszą być szczególnie chronione.

Standardowe środki bezpieczeństwa muszą być ekonomicznie uzasadnione w stosunku do wartości informacji wymagających ochrony oraz systemów teleinformatycznych. Należy zapobiegać przypadkom szkód pociągających za sobą duże skutki finansowe.

Wszyscy pracownicy firmy przestrzegają odpowiednich przepisów prawa (np. ustaw i rozporządzeń dotyczących ochrony danych), wewnętrznych instrukcji proceduralnych i pracy oraz przepisów umownych. Należy unikać negatywnych konsekwencji finansowych i niematerialnych dla firmy i pracowników wynikających z naruszeń prawa i naruszeń umowy.

Wszyscy pracownicy i kierownictwo firmy są świadomi swojej odpowiedzialności w kontaktach z systemami teleinformatycznymi i wspierają strategię bezpieczeństwa najlepiej jak potrafią.

2.1 Cele szczegółowe

Późne lub nieprawidłowe decyzje zarządcze mogą mieć dalekosiężne konsekwencje. Dlatego dostęp do aktualnych danych kontrolnych jest ważny dla kadry zarządzającej przy podejmowaniu ważnych decyzji. Informacjom tym należy zapewnić wysoki poziom bezpieczeństwa pod względem dostępności i integralności.

Przepisy dotyczące ochrony danych oraz interesy naszych pracowników wymagają zapewnienia poufności danych pracowników. Dane osobowe naszych pracowników podlegają zatem wysokiemu poziomowi ochrony poufności. To samo dotyczy danych osobowych naszych partnerów biznesowych.

Dane zapytań i ofert kierowane do i do naszych klientów, a także dane projektowe od naszych klientów i naszego działu rozwoju podlegają bardzo wysokim wymogom poufności. Ich utrata lub kradzież może skutkować niekorzystnymi warunkami konkurencyjnymi lub roszczeniami odszkodowawczymi wobec nas. Środki techniczne i organizacyjne oraz wysoki poziom uwagi ze strony pracowników chronią poufność i zapobiegają manipulacjom.

Dla obszarów logistycznych i zakładów produkcyjnych zapewniona jest dostępność i bezbłędność systemów. Przestoje są dopuszczalne jedynie w bardzo ograniczonym zakresie, ponieważ mogą bezpośrednio i pośrednio prowadzić do zmniejszenia przychodów i mieć negatywny wpływ na zadowolenie klientów.

Wykorzystywanie Internetu i aplikacji portalowych do pozyskiwania informacji i komunikowania się jest dla nas oczywistością. Poczta elektroniczna zastępuje lub uzupełnia inne kanały komunikacji. Odpowiednie środki zapewniają, że ryzyko stosowania pozostaje na możliwie najniższym poziomie.

3. Zarządzanie bezpieczeństwem informacji

Aby osiągnąć cele związane z bezpieczeństwem informacji, utworzono organizację zajmującą się bezpieczeństwem. Powołano inspektora bezpieczeństwa informacji (ISB/CISO). Specjalista ds. bezpieczeństwa informacji na swoim stanowisku podlega bezpośrednio kierownictwu.

Kierownictwo zapewnia inspektorowi bezpieczeństwa informacji wystarczające zasoby finansowe i czasowe, aby móc otrzymywać regularne szkolenia i informacje oraz osiągać cele w zakresie bezpieczeństwa informacji wyznaczone przez kierownictwo.

Administratorzy bezpieczeństwa teleinformatycznego i inspektor bezpieczeństwa informacji muszą w swojej pracy korzystać ze wsparcia specjalistów ds. teleinformatycznych.

Specjalista ds. bezpieczeństwa informacji musi być zaangażowany we wszystkie projekty na wczesnym etapie, aby uwzględnić aspekty związane z bezpieczeństwem w fazie planowania. Jeżeli dotyczy to danych osobowych, to samo dotyczy inspektora ochrony danych.

Użytkownicy ICT mają obowiązek stosować się do poleceń inspektora bezpieczeństwa informacji w kwestiach związanych z bezpieczeństwem.

4. Środki bezpieczeństwa

Za wszystkie procedury, informacje, aplikacje teleinformatyczne i systemy teleinformatyczne wyznaczana jest osoba odpowiedzialna, która we współpracy z inspektorem bezpieczeństwa informacji ustala odpowiednie potrzeby w zakresie ochrony.

Należy wyznaczyć zastępców do wszystkich odpowiedzialnych funkcji. Należy zapewnić poprzez instrukcje i wystarczającą dokumentację, aby przedstawiciele mogli wykonywać swoje zadania.

Budynki i pomieszczenia są chronione odpowiednią kontrolą dostępu. Dostęp do systemów teleinformatycznych chroniony jest odpowiednią kontrolą dostępu, a dostęp do danych – restrykcyjną strategią autoryzacji.

We wszystkich systemach teleinformatycznych stosowane są programy ochrony przed wirusami komputerowymi. Całość dostępu do Internetu jest zabezpieczona odpowiednimi systemami firewall. Wszystkie programy zabezpieczające są konfigurowane i administrowane w taki sposób, aby zapewniały skuteczną ochronę i zapobiegały manipulacjom. Ponadto użytkownicy ICT wspierają te środki bezpieczeństwa poprzez świadomy sposób pracy i informują odpowiednie władze w przypadku jakichkolwiek nieprawidłowości.

Ze wszystkimi systemami teleinformatycznymi, aplikacjami i wszystkimi informacjami należy obchodzić się przy użyciu odpowiednich środków technicznych i organizacyjnych, aby w każdym momencie można było osiągnąć cele ochrony. Środki techniczne i organizacyjne należy regularnie sprawdzać i w razie potrzeby dostosowywać.

Nigdy nie można całkowicie wykluczyć utraty danych. Kompleksowe tworzenie kopii zapasowych danych zapewnia zatem możliwość szybkiego wznowienia operacji ICT w przypadku utraty części danych operacyjnych lub w sposób oczywisty nieprawidłowych. Informacje są spójnie oznakowane i przechowywane w taki sposób, aby można je było szybko znaleźć.

Aby ograniczyć lub zapobiec poważnym szkodom w wyniku sytuacji awaryjnych, należy szybko i konsekwentnie reagować na zdarzenia związane z bezpieczeństwem. Środki nadzwyczajne ujęto w osobnej koncepcji gotowości na wypadek sytuacji awaryjnych. Naszym celem jest utrzymanie krytycznych procesów biznesowych nawet w przypadku awarii systemów i przywrócenie dostępności uszkodzonych systemów w akceptowalnym czasie.

Jeżeli usługi teleinformatyczne zlecamy podmiotom zewnętrznym, szczegółowe wymogi bezpieczeństwa określamy w umowach o gwarantowanym poziomie usług. Jeżeli w celu realizacji umowy konieczne będzie udostępnienie dostawcom danych wymagających wysokiego stopnia ochrony, nałożymy na nich odrębny i wyraźny obowiązek zachowania tajemnicy. Ustanawia się prawo do kontroli.

Użytkownicy ICT biorą udział w szkoleniach z zakresu prawidłowego korzystania z usług ICT i związanych z tym środków bezpieczeństwa. Kierownictwo firmy wspiera szkolenia i dokształcanie oparte na potrzebach.

5. Popraw bezpieczeństwo

System zarządzania bezpieczeństwem informacji jest regularnie sprawdzany pod kątem jego aktualności i efektywności. Ponadto środki są regularnie sprawdzane, aby sprawdzić, czy pracownicy, których dotyczą, są o nich świadomi oraz czy można je wdrożyć i zintegrować z procesem operacyjnym.

Kierownictwo wspiera stałe podnoszenie poziomu bezpieczeństwa. Zachęcamy pracowników do przekazywania ewentualnych ulepszeń lub słabych punktów odpowiednim działom.

Pożądany poziom bezpieczeństwa i ochrony danych zapewniany jest poprzez ciągłą weryfikację regulaminów i ich zgodności. Odchylenia są analizowane w celu poprawy stanu bezpieczeństwa i ciągłego jego aktualizowania o najnowsze technologie bezpieczeństwa teleinformatycznego.

6. Konsekwencje nieprzestrzegania przepisów

Nieprzestrzeganie postanowień niniejszej polityki może mieć poważne konsekwencje dla firmy. Naruszenia tego mogą – w zależności od wagi i okoliczności – skutkować konsekwencjami dyscyplinarnymi lub prawnymi.

7. Odniesienie do Deklaracji Zasad IA

Powyższe wytyczne uzupełniają oświadczenie dotyczące zasad polityki IDEAL Automotive, które jest regularnie przeglądane i dostosowywane, jeśli to konieczne. Wszyscy pracownicy mają obowiązek zapoznania się z aktualną treścią polityki i zapewnienia, że ich postępowanie jest zgodne z zasadami tam określonymi.

8. Procedura zmian

Zmiany w wytycznych dotyczących bezpieczeństwa informacji wprowadzane są systematycznie i przejrzyście. Każda planowana zmiana jest najpierw sprawdzana i zatwierdzana przez kierownictwo ds. bezpieczeństwa informacji. Nowa lub zmieniona treść zostanie zintegrowana z naszym programem szkoleniowym, aby zapewnić zrozumienie i wdrożenie wymagań.

9. Zakres

Niniejsza polityka dotyczy wszystkich pracowników, partnerów zewnętrznych i usługodawców firmy, którzy mają dostęp do informacji i systemów firmy. Obejmuje wszystkie informacje fizyczne i cyfrowe, a także odpowiednie środki techniczne i organizacyjne mające na celu ochronę tych informacji.

Bamberg, 31.10.2024

- Kierownictwo -	- Inspektor ds. bezpieczeństwa informacji -
Stefan Frey	Martin Schnapp

m.schnapp@ideal-automotive.com, Oct 31,2024 09:22:31 AM UTC