POLITYKA CYBERBEZPIECZEŃSTWA
ZAKŁADÓW PORCELANY STOŁOWEJ LUBIANA S.A.

1. Cel i Zakres

Celem niniejszej Polityki Cyberbezpieczeństwa jest zapewnienie ochrony systemów informatycznych, danych oraz zasobów organizacji przed zagrożeniami cybernetycznymi, z uwzględnieniem zasad zrównoważonego rozwoju, etyki cyfrowej oraz zarządzania ryzykiem zgodnie z wytycznymi ESG (Environmental, Social, Governance).

Zakres polityki obejmuje:

- Ochronę systemów IT, aplikacji oraz baz danych.
- Procedury zarządzania incydentami i reagowania na zagrożenia.
- Wymogi dotyczące szkolenia oraz podnoszenia świadomości w zakresie cyberbezpieczeństwa.
- Przeglądy, audyty oraz aktualizacje polityki w celu jej dostosowania do zmieniających się zagrożeń.
- Wdrożenie zasad zrównoważonego IT, ochrony prywatności i zgodności z międzynarodowymi regulacjami.

2. Role i Odpowiedzialności

2.1. Administrator IT

- Odpowiada za utrzymanie, zabezpieczenie i monitorowanie infrastruktury IT.
- Wdraża oraz kontroluje politykę cyberbezpieczeństwa.
- Nadzoruje aktualizacje systemów i aplikacji w celu eliminacji podatności.
- Zapewnia efektywność energetyczną systemów IT oraz minimalizację śladu węglowego organizacji.

2.2. Pracownicy

- Przestrzegają zasad cyberbezpieczeństwa oraz zgłaszają incydenty.
- Korzystają z systemów zgodnie z nadanymi uprawnieniami.
- Uczestniczą w szkoleniach i testach związanych z cyberbezpieczeństwem.
- Zobowiązani do ochrony danych osobowych oraz etycznego korzystania z narzędzi cyfrowych.

2.3. Dział IT

- Wdraża politykę cyberbezpieczeństwa oraz przeprowadza audyty.
- Reaguje na incydenty i analizuje nowe zagrożenia.
- Współpracuje z administratorem IT w zakresie podnoszenia poziomu bezpieczeństwa.
- Zapewnia zgodność z regulacjami RODO, oraz najlepszymi praktykami w zakresie ESG.

3. Zasady Bezpieczeństwa

3.1. Kontrola Dostępu

- Każdy użytkownik posiada unikalne konto z minimalnymi wymaganymi uprawnieniami.
- Obowiązkowe stosowanie silnych haseł (minimum 8 znaków, zawierających duże i małe litery, cyfry oraz znaki specjalne) oraz ich regularna zmiana.
- Dwuetapowa autoryzacja (MFA) dla dostępu do krytycznych systemów.
- Automatyczne blokowanie konta po określonej liczbie nieudanych prób logowania.

3.2. Ochrona Sieci

- Wdrożenie zapór ogniowych oraz systemów wykrywania i zapobiegania włamaniom (IDS/IPS).
- Szyfrowanie komunikacji wewnętrznej i zewnętrznej.
- Monitorowanie ruchu sieciowego oraz wykrywanie anomalii.
- Segmentacja sieci w celu ograniczenia możliwości rozprzestrzeniania się zagrożeń.

- Stosowanie rozwiązań energooszczędnych oraz zmniejszenie zużycia zasobów.

3.3. Ochrona Danych

- Regularne tworzenie kopii zapasowych i ich przechowywanie w bezpiecznych lokalizacjach.
- Szyfrowanie wrażliwych danych oraz stosowanie polityki minimalizacji przechowywania danych.
- Ograniczenie dostępu do danych na zasadzie "najmniejszych uprawnień" (PoLP).
- Regularne testy integralności kopii zapasowych.

4. Zarządzanie Incydentami

- Każdy incydent cyberbezpieczeństwa musi być natychmiast zgłoszony do działu IT.
- Procedura reagowania obejmuje: identyfikację incydentu, analizę, ograniczenie skutków, przywrócenie działania systemów oraz raportowanie.
- Regularne testy i symulacje reagowania na incydenty.
- Wdrażanie środków zapobiegawczych po każdym incydencie w celu minimalizacji ryzyka ponownego wystąpienia.

5. Szkolenia i Świadomość

- Obowiązkowe szkolenia z zakresu cyberbezpieczeństwa dla wszystkich pracowników, dostosowane do ich zakresu obowiązków.
- Regularne aktualizacje polityki bezpieczeństwa oraz informowanie o nowych zagrożeniach.
- Organizowanie kampanii uświadamiających dotyczących phishingu, malware oraz metod socjotechnicznych stosowanych przez cyberprzestępców.
- Promowanie zasad etycznego korzystania z technologii i ochrony prywatności.

6. Audyty i Przeglądy

- Regularne audyty bezpieczeństwa systemów IT przeprowadzane przez niezależnych specjalistów.
- Przegląd polityki cyberbezpieczeństwa co najmniej raz w roku lub po wystąpieniu istotnych zmian w organizacji.
- Analiza podatności i przeprowadzanie testów penetracyjnych w celu identyfikacji potencjalnych luk w zabezpieczeniach.

7. Postanowienia Końcowe

- Naruszenie polityki cyberbezpieczeństwa może skutkować konsekwencjami dyscyplinarnymi, w tym rozwiązaniem stosunku pracy.
- Polityka wchodzi w życie z dniem zatwierdzenia przez Zarząd i podlega okresowym aktualizacjom zgodnie z obowiązującymi przepisami prawa oraz najlepszymi praktykami w zakresie cyberbezpieczeństwa i ESG.