

Obszar: Bezpieczeństwo Informatyczne

Koordynator Obszaru: Dyrektor Działu IT

Dokumenty związane: Polityka Bezpieczeństwa Informatycznego

Zasady Bezpieczeństwa dla Dostawców Grupy QEMETICA (wersja 0.01) („Zasady”)

I. Zasada świadomości zagrożeń i zapewnienia wymaganego poziomu ochrony

Dostawca musi zapewnić, że zadania realizowane na rzecz Grupy QEMETICA będą wykonywane zgodnie z najlepszymi praktykami określonymi w PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Identyfikacji celów bezpieczeństwa dla realizowanej usługi
- b. Szacowania ryzyka związanego z realizacją usługi
- c. Wdrożenia i stosowania zabezpieczeń adekwatnych do zidentyfikowanych ryzyk
- d. Zapewnienia ciągłości działania w zakresie realizowanej usługi
- e. Zapewnienia kontroli nad personelem realizującym usługę

II. Zasada ochrony danych osobowych

Dostawca musi spełnić wymagania dotyczące bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych wynikające wprost z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

III. Zasada nadzoru nad oprogramowaniem produkcyjnym

Dostawca musi zapewnić nadzór nad oprogramowaniem produkcyjnym zgodnie z wytycznymi określonymi w rozdz. 12.5 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Wszędzie tam, gdzie występuje wpływ na ciągłość działania krytycznych procesów biznesowych i produkcyjnych Grupy QEMETICA, uzgodnienia z Grupą QEMETICA procedur instalacyjnych i procedur powrotu („roll-back”) w przypadku niepowodzenia wprowadzanej zmiany lub podejmowanego działania utrzymaniowego
- b. Aktualizowania oprogramowania produkcyjnego, aplikacji i bibliotek
- c. Zarządzanie wersjonowaniem oprogramowania
- d. Wdrażania zmian w oprogramowaniu produkcyjnym po pozytywnych testach bezpieczeństwa, integracyjnych, wydajnościowych, funkcjonalnych, regresyjnych
- e. Pozyskiwania informacji o podatnościach technicznych utrzymywanych lub rozwijanych systemów informatycznych i rekomendowanie Grupie QEMETICA odpowiednich środków w celu ich mitygacji

IV. Zasada bezpiecznej eksploatacji

Dostawca musi zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji zgodnie z wytycznymi określonymi w rozdz. 12 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Posiadania i na bieżąco aktualizowania dokumentacji systemowej zawierającej:
 - Specyfikację komponentów sprzętowych środowiska
 - Specyfikację komponentów programowych środowiska
 - Specyfikację kont technicznych
 - Specyfikację usług
- b. Posiadania i na bieżąco aktualizowania procedur eksploatacyjnych zawierających instrukcję realizacji zadań w zakresie:
 - Instalacji i konfiguracji systemów
 - Procedur wykonywania, testowania i przywracania kopii zapasowych
 - Procedur zarządzania zmianą
 - Procedur zarządzania pojemnością
 - Procedur ponownego uruchamiania i odtwarzania systemu po awarii
 - Procedur monitorowania i diagnozowania problemów
 - Procedur serwisowych na wypadek awarii

V. Zasada bezpiecznego łańcucha dostaw

Dostawca musi zidentyfikować łańcuch dostaw związany z realizacją usług na rzecz Grupy QEMETICA i zapewnić jego bezpieczeństwo zgodnie z wymaganiami określonymi w rozdz. 14.2.7 i 15.1.3 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Identyfikacji ryzyk w łańcuchu dostaw
- b. Nadzorowania i monitorowania realizacji usług zleconym podmiotom zewnętrznym

VI. Zasada bezpiecznego personelu

Dostawca musi zapewnić bezpieczeństwo personelu zgodnie z najlepszymi praktykami określonymi w rozdz. 7.2.1, 7.2.2 oraz 7.3.1 normy PN-ISO/IEC 27002-17, adekwatnie do zadań realizowanych na rzecz Grupy QEMETICA. W szczególności Dostawca jest zobowiązany do:

- a. Przekazania personelowi, realizującemu usługi na rzecz Grupy QEMETICA, informacji o wymaganiach bezpieczeństwa współpracy z Grupą QEMETICA
- b. Zapewnienia, poprzez adekwatne szkolenia, odpowiedniego poziomu świadomości o zagrożeniach, wymaganiach bezpieczeństwa Grupy QEMETICA i zasad bezpiecznej realizacji usługi
- c. Prowadzenia rejestru oświadczeń o zapoznaniu się z wymaganiami bezpieczeństwa i odpowiednimi politykami ich realizacji, podpisanych przez personel. Podpisane oświadczenie powinno także zawierać klauzulę o zachowaniu poufności pozyskanych informacji

VII. Zasada bezpieczeństwa zasobów chmury obliczeniowej

Dostawca musi stosować się do zakazu zapisywania oraz kopiowania jakichkolwiek informacji z zasobów chmury obliczeniowej Grupy QEMETICA na służbowe lub prywatne zasoby w tym (i) komputery, (ii) fizyczne zewnętrzne nośniki danych, (iii) pamięci przenośne, (iv) urządzenia mobilne, (v) konta pocztowe, (vi) i inne nie wymienione środki nie będące własnością Grupy QEMETICA.

VIII. Zasada bezpieczeństwa urządzeń przenośnych

Dostawca musi zapewnić bezpieczeństwo wykorzystywanych urządzeń przenośnych zgodnie z najlepszymi praktykami określonymi w rozdz. 6.2.1 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Zapewnienia bezpieczeństwa urządzeń przenośnych w sieciach niezauważanych
- b. Zapewnienia kontroli nad urządzeniami przenośnymi
- c. Zapewnienia rozliczalności działań podejmowanych na urządzeniach przenośnych

IX. Zasada bezpieczeństwa zewnętrznych nośników danych

Dostawca powinien ograniczyć użycie zewnętrznych nośników danych, a w przypadku ich uzasadnionego użycia musi zapewnić bezpieczeństwo nośników wykorzystywanych w związku z realizacją usług na rzecz Grupy QEMETICA zgodnie z najlepszymi praktykami określonymi w rozdz. 8.3 normy PN-ISO/IEC 27002-17. W szczególności Dostawca jest zobowiązany do zapewnienia szyfrowania nośnika, dopuszczonego do użytku w związku ze świadczeniem usług.

X. Zasada bezpieczeństwa powierzonych zasobów

Dostawca musi zapewnić bezpieczne i właściwe użycie powierzonych zasobów, wykorzystywanych do realizacji usług na rzecz Grupy QEMETICA, zgodnie z najlepszymi praktykami określonymi w rozdz. 8.1.3

i 8.1.4 normy PN-ISO/IEC 27002-17. W szczególności Dostawca jest zobowiązany do:

- a. Wdrożenia zasad akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji
- b. Zapewnienia kontroli nad powierzonymi zasobami i odpowiedniego poziomu ochrony adekwatnego do specyfiki realizowanej usługi na rzecz Grupy QEMETICA
- c. Zwrócenia po zakończeniu wykonywanej usługi, wszelkich powierzonych zasobów w tym informacji, a po ich przekazaniu do Grupy QEMETICA, bezpowrotne zniszczenie po upływie uzgodnionego okresu retencji danych

XI. Zasada bezpieczeństwa pracy zdalnej

Dostawca musi zapewnić bezpieczeństwo pracy zdalnej zgodnie z najlepszymi praktykami określonymi w rozdz. 6.2.2 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Zapewnienia bezpieczeństwa pracy zdalnej
- b. Zapewnienia kontroli nad pracą zdalną

- c. Zapewnienia rozliczalności działań podejmowanych w ramach pracy zdalnej
- d. Realizacji zdalnego dostępu do zasobów Grupy QEMETICA, wyłącznie z wykorzystaniem autoryzowanych kanałów komunikacji
- e. Realizacji zdalnego dostępu do zasobów Grupy QEMETICA tylko w celach i zakresie realizowanej usługi
- f. Grupa QEMETICA ma prawo do nagrywania, przechowywania i wykorzystania w celach dowodowych nagrań z przeprowadzonego zdalnego dostępu
- g. Grupa QEMETICA ma prawo do rejestrowania, przechowywania i wykorzystania w celach dowodowych wszelkich zdarzeń związanych z realizacją zdalnego dostępu

XII. Zasada bezpieczeństwa procesu projektowego

Dostawca musi wykorzystywać w procesach projektowych, najlepsze praktyki określone w rozdz. 14.2.1, 14.2.2, 14.2.5 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Projektowania i wdrażania zabezpieczeń w całym cyklu realizacji usługi lub cyklu życia systemu informatycznego
- b. Nadzorowania i rejestrowania zmian w systemach, podczas ich cyklu rozwojowego, z zastosowaniem formalnych procedur kontroli zmian
- c. Projektowania systemów informatycznych w oparciu o ustanowione i udokumentowane zasady projektowania bezpiecznych systemów oraz stosowanie ich do wszystkich prac implementacyjnych nad systemami informatycznymi

XIII. Zasada zarządzania zmianą

Dostawca musi zapewnić, że zmiany wprowadzane do projektowanych rozwiązań będą realizowane zgodnie z najlepszymi praktykami określonymi w rozdz. 15.2.2 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do :

- a. Stosowania procesu zarządzania zmianą
- b. Rejestrowania zmian i prowadzenia rejestru zmian
- c. Zapewnienia, że zmiany będą autoryzowane przez upoważnione osoby

XIV. Zasada zarządzania incydentami bezpieczeństwa

Dostawca musi zapewnić identyfikowanie i obsługę incydentów bezpieczeństwa zgodnie z najlepszymi praktykami określonymi w rozdz. 16.1 normy PN-ISO/IEC 27002-17. W szczególności Dostawca jest zobowiązany do niezwłocznego formalnego zgłaszania do Grupy QEMETICA wszelkich incydentów bezpieczeństwa związanych z realizacją usługi na rzecz Grupy QEMETICA, a w przypadku zaistnienia incydentu bezpieczeństwa Dostawca musi podjąć wszelkie niezbędne środki, aby zminimalizować wpływ i zasięg incydentu oraz zabezpieczyć materiał dowodowy.

XV. Zasada bezpieczeństwa środowisk rozwojowych

Dostawca musi realizować prace rozwojowe z wykorzystaniem bezpiecznego środowiska rozwojowego, dla którego najlepsze praktyki określono w rozdz. 14.2.6 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do:

- a. Zabezpieczenia środowiska rozwojowego adekwatne do poziomu ryzyka związanego z wykorzystaniem danych o określonym poziomie ochrony
- b. Zapewnienia przepływu danych od i do środowiska rozwojowego, zapewniając brak upływu danych testowych oraz brak nieuprawnionego dostępu do systemów

XVI. Zasada bezpieczeństwa środowisk testowych

Dostawca musi zapewnić bezpieczeństwo środowisk testowych zgodnie z najlepszymi praktykami określonymi w rozdz. 14.3 normy PN-ISO/IEC 27002-17, w szczególności Dostawca powinien zapewnić ochronę środowisk i danych testowych na adekwatnym do zidentyfikowanych ryzyk poziomie.

XVII. Zasada zarządzania uprawnieniami

Dostawca musi zarządzać uprawnieniami dostępu do własnych środowisk zgodnie z najlepszymi praktykami określonymi w rozdz. 9.2, 9.3, 9.4 normy PN-ISO/IEC 27002-17. W zakresie środowisk informatycznych Grupy QEMETICA, Dostawca jest zobowiązany do:

- a. Nie dokonywania żadnych zmian w zakresie dostępu i uprawnień bez autoryzacji Grupy QEMETICA
- b. Stosowania zasady minimalnego wymaganego zakresu dostępu i uprawnień

Dostawca ponadto, musi stosować zasady wnioskowania o uprawnienia, obowiązujące w Grupie QEMETICA

i wprowadzające podział na:

- a. Dostęp podstawowy, rozumiany jako dostęp i uprawnienia do usług tożsamości i usług biurowych, na którą mogą składać się: konto domenowe, aplikacje biurowe, poczta elektroniczna
- b. Dostęp rozszerzony, rozumiany jako dostęp i uprawnienia do wszystkich innych usług

Dostęp podstawowy i rozszerzony jest nadawany na podstawie zgłoszenia w systemie informatycznego wsparcia użytkownika, zainicjowanego przez pracownika/przełożonego pracownika lub współpracownika Grupy QEMETICA nadzorującego realizację umowy z Dostawcą.

XVIII. Zasada separacji środowisk rozwojowych i testowych

Dostawca musi zapewnić (co najmniej na poziomie maszyny wirtualnej lub fizycznej) separację środowisk przeznaczonych do realizacji usług na rzecz Grupy QEMETICA od środowisk realizujących zadania dla innych klientów, zgodnie z najlepszymi praktykami określonymi w rozdz. 12.1.4 normy PN-ISO/IEC 27002-17.

XIX. Zasada ochrony kopii zapasowych

Dostawca musi zapewnić ochronę kopii zapasowych danych przetwarzanych w trakcie realizacji usługi na rzecz Grupy QEMETICA, zgodnie z najlepszymi praktykami określonymi w rozdz. 12.3 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do zapewnienia szyfrowanych kopii zapasowych.

XX. Zasada zapewnienia bezpieczeństwa kodów źródłowych

Dostawca musi zapewnić bezpieczeństwo repozytorium kodów źródłowych, zgodnie z wytycznymi określonymi w rozdz. 9.4.5 normy PN-ISO/IEC 27002-17, w szczególności Dostawca jest zobowiązany do zapewnienia kontroli i rozliczalności dostępu do repozytorium kodów źródłowych.