

## **Systemy ochrony danych i zbiorów dla Centrali i Oddziału GDDKiA w Warszawie**

### **I. Postanowienia ogólne**

System określa zasady zabezpieczenia i ochrony danych księgowych, programów i nośników komputerowych, stosowanych przy eksploatacji systemów informatycznych F/K (finansowo - księgowych) i podsystemów współpracujących z tymi systemami, które są wyszczególnione w ust. 1 załącznika nr 4 do zarządzenia.

Niniejszy system ma zastosowanie do wszystkich użytkowników systemów informatycznych i podsystemów współpracujących z tymi systemami, o których mowa powyżej.

### **II. Słownik użytych pojęć i skrótów**

Użyte pojęcia i skróty oznaczają:

- 1) **ERP - planowanie zasobów przedsiębiorstwa** (ang. Enterprise Resource Planning, tłumaczone przez producentów też jako zaawansowane zarządzanie zasobami) – określenie klasy systemów informatycznych służących wspomaganie zarządzania przedsiębiorstwem lub współdziałania grupy współpracujących ze sobą przedsiębiorstw, poprzez gromadzenie danych oraz umożliwienie wykonywania operacji na zebranych danych. Wspomaganie to może obejmować wszystkie lub część szczebli zarządzania i ułatwia optymalizację wykorzystania zasobów przedsiębiorstwa oraz zachodzących w nim procesów. Systemy ERP są oprogramowaniem modułowym, tj. składają się z niezależnych od siebie choć współpracujących ze sobą aplikacji i są zaliczane do klasy zintegrowanych systemów informatycznych;
- 2) **SAP AG** (niem. Systemanalyse und Programmentwicklung, ang. Systems Applications and Products in Data Processing) – międzynarodowe przedsiębiorstwo informatyczne założone w 1972 r. z siedzibą w Walldorf w Niemczech. SAP jest dostawcą oprogramowania biznesowego ERP dla przedsiębiorstw ze wszystkich branż i sektorów gospodarki;
- 3) **kopia bezpieczeństwa** (ang. backup copy) – w informatyce dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.

Proces wykonywania kopii bezpieczeństwa, w odniesieniu do kopii długotrwałych, jest nazywany archiwizacją;

Ze względu na archiwizowane dane wyróżnia się trzy metody wykonywania kopii bezpieczeństwa:

- a) backup pełny (image) - archiwizacja wszystkich danych, niezależnie od czasu kiedy były archiwizowane poprzednio,
  - b) backup przyrostowy - archiwizowane są tylko pliki zmienione od ostatniego backup'u pełnego lub przyrostowego,
  - c) backup różnicowy - archiwizowane są tylko pliki zmienione od ostatniego pełnego backup'u. Backup różnicowy i przyrostowy zawsze łączony jest z backup'em pełnym;
- 4) **Redo Logi** - przetwarzanie transakcyjne w bazach danych Oracle polega na zapisywaniu efektów działania poleceń wchodzących w skład transakcji do buforów dziennika powtórzeń (redo log buffer), a w następnej kolejności do plików dziennika powtórzeń (redo logs), buforów danych (data file buffer) i plików bazodanowych (data files). "Redologi" (\*.log) rejestrują wszystkie zatwierdzone (commit) transakcje bazy danych czyli te operacje które coś zmieniają w bazie. Standardowo po instalacji bazy są trzy grupy plików redo logs o określonej wielkości. Jeśli pierwszy z plików się zapełni transakcje zapisywane są do następnego pliku i tak w koło;
- 5) **AID** (ang. Redundant Array of Independent Disks, Nadmiarowa macierz niezależnych dysków) – polega na współpracy dwóch lub więcej dysków twardych w taki sposób, aby zapewnić dodatkowe możliwości, nieosiągalne przy użyciu jednego dysku jak i kilku dysków podłączonych jako oddzielne.
- RAID używa się w następujących celach:
- a) zwiększenie niezawodności (odporność na awarie),
  - b) zwiększenie wydajności transmisji danych,
  - c) powiększenie przestrzeni dostępnej jako jedna całość.

### III. Stosowane środki ostrożności

1. W celu zapobieżenia istniejącym zagrożeniom danych księgowych, przetwarzanych za pomocą techniki komputerowej, dane znajdujące się w zasobach systemu ERP archiwizowane są przy użyciu oprogramowania Symantec Backup Exec w wersji 2010 R3 Version 13.0 Rev. 5204 oraz za pomocą mechanizmów wbudowanych w system SAP w następujący sposób:
  - 1) codziennie wykonywana jest pełna kopia bazy danych systemu PRD (system produkcyjny) najpierw na wydzielony zasób dyskowy, a następnie

- na taśmy magnetyczne LTO3. Biblioteka zawierająca taśmy znajduje się w serwerowni w siedzibie Centrali GDDKiA;
- 2) serwer PRD (produkcyjny) – backup systemu operacyjnego wykonywany jest w razie potrzeby (np. po instalacji poprawek systemowych) oraz na koniec roku jako pełen backup (image), kopia bazy danych wraz z redo logami jest archiwizowana na żądanie wydziału finansowego np. po zamknięciu roku obrotowego i zanoszona do sejfu w wydzielonym pomieszczeniu;
  - 3) serwery EDEV, EQAS, BDEV, BQAS, BPRD, SMP – backup systemu operacyjnego jest realizowany w razie potrzeby jako pełny (image), kopia bazy danych oraz Redo Logi są archiwizowane codziennie jako pełny backup (full backup);
  - 4) archiwizacja bazy danych Oracle serwera PRD, wykonywana jest codziennie jako pełen Backup (full backup) wraz z kopią Archive Log;
  - 5) w backupie danych ERP pośredniczy macierz CLUSTERERP, producent: DELL model Compellent SC040, wyposażona w 15 dysków SAS 600GB 15k rpm oraz 9 dysków SAS 2TB 7,2k rpm;
  - 6) fizycznie dane przechowywane w zasobach pamięci masowej są składowane w bibliotece taśmowej i znajdują się w wydzielonym do tego celu pomieszczeniu GDDKiA, które posiada niezbędne zabezpieczenia w celu ochrony danych;
  - 7) nośniki zawierające zarchiwizowane dane miesięczne, przechowywane są zamknięte w osobnym, wydzielonym do tego celu pomieszczeniu GDDKiA. Dodatkowo dane są przechowywane w sejfie, do którego klucz posiadają administratorzy systemowi;
  - 8) płyty instalacyjne stosowanych systemów oraz systemów współpracujących z programami, z wyłączeniem systemów, dla których środowiskiem eksploatacyjnym jest Internet, przechowywane są w okresie korzystania oraz przez 5 lat po terminie zaprzestania z ich korzystania.
2. Pomieszczenie serwerowni, o którym mowa w ust. 1 pkt 1, chronione jest za pomocą systemu do kontroli dostępu, gdzie wstęp mają tylko upoważnieni administratorzy (pomieszczenie zabezpieczone jest również w instalację alarmową, przeciwpożarową (system gaszenia gazem), oraz w cztery klimatyzatory).
3. Zabezpieczenia przed utratą danych:
- 1) system finansowo - księgowy SAP PRD umieszczony jest na dwóch różnych serwerach pracujących w klastrze MSCS Active/Passive (w momencie awarii jednego z serwerów, automatycznie system przenoszony jest na drugi serwer);

- 2) baza danych umieszczona jest na macierzy dyskowej, która skonfigurowana jest w tzw. RAID'zie (10 oraz 5) (awaria pojedynczego dysku nie powoduje przerwy w funkcjonowaniu systemu, rolę uszkodzonego dysku przejmuje tzw. dysk HotSpare);
  - 3) codziennie wykonywana jest pełna kopia bazy danych na taśmy LTO3;
  - 4) w zależności od potrzeb, wykonywana jest kopia dodatkowa na taśmę LTO3 i zanoszona do sejfu w wydzielonym pomieszczeniu (np. na koniec roku);
  - 5) serwery podłączone są do centralnego UPS-a, który umożliwia działanie systemów w przypadku zaniku zasilania.
4. Służby informatyczne zobowiązane są do:
- 1) ustalenia zasad korzystania z haseł dostępu do systemu dla poszczególnych pracowników;
  - 2) organizowania przeglądów i bieżącej konserwacji sprzętu komputerowego wraz ze składnikami peryferyjnymi;
  - 3) konserwacji standardowego oprogramowania, poprzez poszukiwanie nowych, bardziej sprawnych i pozbawionych wcześniejszych błędów wersji programów;
  - 4) zapewnienia ochrony przed wirusami komputerowymi, poprzez zakup i bieżącą aktualizację programów antywirusowych;
  - 5) określenia zasad współpracy z zewnętrznymi serwisantami, eliminujące długotrwałe przerwy w pracy systemu;
  - 6) kontroli antywirusowej wszystkich zewnętrznych nośników dołączonych do infrastruktury.
5. Pracownik korzystający z systemu finansowo - księgowego SAP, nie może pozostawić włączonego komputera z uruchomionym systemem, w czasie swojej nieobecności w pomieszczeniu, w którym pracuje.

#### **IV. Przechowywanie dokumentacji finansowo - księgowej**

1. W zakresie sposobu i okresu przechowywania ksiąg rachunkowych, dowodów księgowych, dokumentów inwentaryzacyjnych i sprawozdań finansowych oraz zbiorów danych, stosuje się zasady archiwizacji tego rodzaju dokumentacji, które wynikają z obowiązujących w tym zakresie uregulowań wewnętrznych, przepisów ustawy o rachunkowości oraz ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych.

2. Dowody księgowe i dokumenty inwentaryzacyjne za bieżący i poprzedni rok obrotowy, przechowywane są w pomieszczeniach właściwych komórek finansowo - księgowych GDDKiA.
3. Dla dokumentów finansowo - księgowych, dotyczących rozliczenia środków finansowych pochodzących z Unii Europejskiej, stosuje się następujące zasady:
  - 1) w zakresie Sektorowego Programu Operacyjnego Transport (SPOT):
    - a) okres przechowywania dokumentów dotyczących wydatków i kontroli związanych z Sektorowym Programem Operacyjnym Transport na lata 2004-2006 wynosi 3 lata, licząc od dnia otrzymania przez Rzeczpospolitą Polską płatności końcowej z Komisji Europejskiej,
    - b) w przypadku projektów, przy realizacji, których korzystano z pomocy publicznej (Dzianie 1.3 - Regionalna infrastruktura społeczna), okres przechowywania dokumentacji wynosi 10 lat, licząc od dnia przyznania ostatnich środków w ramach pomocy publicznej;
  - 2) w zakresie Funduszu Spójności i TEN-T:
    - a) okres przechowywania dokumentów wynosi 3 lata, o ile dwustronne ustalenia administracyjne nie stanowią inaczej, od wypłaty przez komisję końcowego salda w ramach projektu,
    - b) archiwizacja dla perspektywy 2007-2013 wynosi 10 lat od momentu udzielenia pomocy, o ile przepisy krajowe nie zakładają dłuższego okresu przechowywania dla poszczególnych dokumentów, tj.:
      - faktur i innych dokumentów potwierdzających poniesione wydatki,
      - ksiąg rachunkowych,
      - wyciągów z kont bankowych (subkont projektów),
      - raportów i dokumentów potwierdzających zawarte w raportach informacje;
  - 3) w zakresie Programu Operacyjnego i Programu Technicznego Infrastruktura i Środowisko (POIiŚ) - archiwizacja wszelkich danych związanych z realizacją Projektu, w szczególności dokumentacji związanej z zarządzaniem finansowym, technicznym, procedurami zawierania umów z wykonawcami, powinna gwarantować należyte bezpieczeństwo przechowywanych danych. Zgodnie z zapisami Umowy o dofinansowanie, okres przechowywania dokumentów finansowo - księgowych wynosi co najmniej 3 lata od daty zamknięcia POIiŚ.

Zastępca Dyrektora  
Biura Ekonomiczno-Finansowego  
GDDKiA

Katarzyna Gnyp

2010-08-20

