Комисия за финансов надзор

ИЗИСКВАНИЯ

за създаване и поддръжка на информационна система на пенсионноосигурително дружество, утвърдени с решение № 568-ПОД от 30.12.2003 г. на заместник-председателя на Комисията за финансов надзор, ръководещ управление «Осигурителен надзор»

I. Общи изисквания

1. Пенсионноосигурителните дружества са длъжни да спазват основните изисквания към информационната им система (ИС), по отношение на нейната надеждност, сигурност, защита от неоторизиран достъп до информационните масиви и възстановяване на информационните процеси след срив.

2. Пенсионноосигурителните дружества сами определят доставчиците на хардуер, разработчиците на софтуер и размера на финансовите средства за изграждане на информационна система и следване на политика на сигурност.

3. Системният и приложен софтуер, използван при разработване и експлоатация на информационната система, трябва да осигурява висока сигурност и надеждност.

4. Информационната система трябва да предоставя възможност за извлечение от индивидуалната осигурителна партида във всеки един момент, както и изготвяне в електронен формат на изискваните от надзорния орган отчети и справки ежедневно, ежемесечно, на тримесечие, полугодие, годишно и при поискване. Файловият формат на отчетите и справките се задава от надзорния орган.

5. Пълното актуално състояние на индивидуалната партида трябва да е достъпно текущо (онлайн) за период от три години назад, а цялата детайлна история на партидата да е достъпна чрез възстановяване от архив за срок не по-голям от 3 часа.

6. Към информационната система следва да могат да се добавят други компоненти (модули) в съответствие с действащата нормативна уредба, както и такива, зададени от пенсионноосигурителното дружество.

7. Пенсионноосигурителните дружества трябва да разполагат с достатъчен брой кадри, притежаващи квалификация и професионален опит, които дават гаранция за ефективно изпълнение на задълженията, свързани с обслужване на информационната система.

8. Пенсионноосигурителните дружества следва да приемат и спазват вътрешни правила за защита на информационните ресурси (политика по управление на сигурността). Всички потребители на ИС трябва да бъдат запознати с вътрешните правила срещу подпис.

II. Изисквания към хардуера и софтуера

1. Инсталираното оборудване – сървър (сървъри) и работни станции да бъде достатъчно надеждно и отказоустойчиво и да има капацитет за максимален възможен брой обслужвани лица.

2. Инсталираното структурно окабеляване (в т.ч. пасивно и активно оборудване) да бъде достатъчно надеждно и отказоустойчиво и да бъде физически разделено.

3. Наличие на допълнително оборудване (климатична инсталация, детектори за дим и температура, алармена инсталация, непрекъсваеми токозахранващи устройства /UPS/).

4. Поддръжка на подробен инвентарен списък на използвания хардуер, софтуер и комуникационно оборудване. Наличие на програма за поддръжка на хардуерни елементи. Наличие на стратегия за развитие.

5. При използване и/или разработване на информационната си система и друг системен или приложен софтуер пенсионноосигурителните дружества трябва да спазват Закона за авторското право, както и приложимите по българското законодателство международни актове за интелектуалната собственост.

III. Функционални изисквания към информационната система

Информационната система за администриране на пенсионни фондове, управлявани от пенсионноосигурително дружество, трябва да съдържа и поддържа в актуално състояние следните основни компоненти за всеки управляван фонд за допълнително пенсионно осигуряване:

1. Регистър на:

1.1. осигурителни договори – в т. ч. по видове за доброволния фонд (договор с лични вноски, договор с работодател или с лице по чл. 230, ал. 3, т. 3 от Кодекса за социално осигуряване (КСО) и договор с друг осигурител);

1.2. на служебно разпределените лица с номер и дата на протокола за служебно разпределение;

1.3. пенсионни договори;

1.4. договори за разсрочено изплащане на натрупаните средства по индивидуалните партиди.

2. Регистър на индивидуалните партиди на осигурените лица и пенсионерите, който трябва да съдържа данните съгласно чл. 24 и чл. 25 от Наредба № 10 от 26.11.2003 г. на Комисията за финансов надзор (КФН), както и партидата на резерва за гарантиране на минималната доходност по чл. 193, ал. 7 от КСО.

3. Регистър на всички постъпили молби за изтегляне или изплащане на средства поотделно за всеки управляван фонд.

4. Регистри по чл.20 от Наредба № 3 от 24.09.2003 г. на КФН.

5. Регистър на постъпилите молби за прехвърляне на средства от една осигурителна партида в друга на един и същи пенсионен фонд на съпруг(а) или на роднини по права линия до втора степен.

6. Регистър на притежаваните от всеки управляван фонд активи, съответстващ на регистъра, воден от банката-попечител и допълнен със записи за оценка на всеки актив.

IV. Изисквания за сигурност и надеждност на информацията

Информационната система трябва да притежава многослойна архитектура за сигурност и да отговаря на следните основни изисквания:

1. Защита на достъпа до данни и приложения чрез хардуерни и софтуерни решения, детайлен одитинг (процес на регистриране, анализ и проверка на всяка дейност, извършвана в системата), контрол на достъпа чрез оторизация и автентификация на потребителите. Пенсионноосигурителното дружество трябва да притежава официален e-mail адрес за контакти и mail сървър, през който да минава обменът на официалната му кореспонденция. E-mail адресът и mail сървърът трябва да са записани в публичния регистър на Комисията за финансов надзор.

2. Физически контрол на достъпа до информационните ресурси в т.ч. охрана, алармени системи, средства за идентификация на входа на сградата и компютърната (сървърна) зала, системи за наблюдение и контрол.

3. Отказоустойчивост на информационната система, реализирана чрез хардуерни решения, инсталиране на надеждни UPS системи, дублиране на устройства, връзки и захранвания на локалната мрежа.

4. Повишена надеждност чрез архивиране на данните. Система и процедури за архивиране. Наличие на алтернативно място за съхранение на информация, което да бъде физически разположено извън основното място на ИС (друга сграда или друг град).

5. План за възстановяване на информационните процеси след срив на системата (природни бедствия, аварии и др.). Възстановяване на данни и процедури. Познаване на плана за възстановяване след срив на системата от страна на персонала. Срокът за възстановяване на основните функции на информационната система трябва да е до 72 часа.

6. Обучение и подготовка на потребителите за работа с информационната система. Запознаване на потребителите с политиката и процедурите за сигурност.