Заявление о применимости

A. Руководство Биржи Международного финансового центра «Астана» (далее- AIX) признает важность информационной безопасности и кибербезопасности как неотъемлемой части деятельности AIX, и обязуется внедрять и соблюдать положения законов, нормативных актов и таких стандартов как ISO 27001, ISO 27032, ISO 27018 и ISO 27018.

B. Руководство и сотрудники AIX обязуются проявлять лояльность по отношению к компании и защищать известную им и находящуюся в их распоряжении информацию от повреждения и от воздействия каких-либо неавторизованных сторон, как внутренних, так и внешних.

C. Руководство AIX выделит необходимые ресурсы на реализацию процессов и инструментов, требуемых и определенных в Политике AIX в области конфиденциальности, а также информационной кибербезопасности и вытекающих из процедур в области кибербезопасности и информации, а также в соответствии с требованиями законодательства в сфере информационной безопасности.

D. Руководство AIX определит уровень информационной безопасности и кибербезопасности, установит степень секретности баз данных и систем, который будет определен в соответствии с наивысшим уровнем секретности доступной информации и по принципу «самых строгих ограничений».

E. Руководство AIX несет ответственность за защиту информационных ресурсов, обеспечивая надлежащую, безопасную и непрерывную работу инфраструктуры, а также за поддержку целостности и доступности информации, хранящейся в различных системах.

F. Руководство AIX несет ответственность за разработку принципов информационной и кибербезопасности, включая любые аспекты, необходимые в процессах и инструментах, внедренных для операционных систем, программного обеспечения и для всех информационных ресурсов, в которых хранится и/или обрабатывается информация.

G. Руководство AIX определит для каждого сотрудника компании категории секретности, относящиеся к их должностным обязанностям, уровню чувствительности и секретности информации, с которой они работают. Кроме того, руководство AIX внедрит процедуры, направленные на контроль и проверку надежности и добросовестного отношения сотрудников AIX к своей работе. Аналогичные процедуры будут предусмотрены и для сотрудников компаний-третьих лиц.

H. Руководство AIX несет ответственность за реализацию требований Политики сотрудниками AIX и партнёрами, и обязуется непрерывно повышать уровень осведомленности среди сотрудников об информационной и кибербезопасности, рисках и угрозах для информации AIX.

I. Руководство AIX разработает процедуры контроля для обеспечения соблюдения компанией, ее сотрудниками и компаниями-третьими лицами требований законодательства, правил, стандартов и процедур.

J. Руководство AIX определит и изложит принципы, процессы и инструменты, необходимые для резервного копирования, восстановления и аварийного восстановления.

K. Руководство AIX установит конкретные задачи и ключевые показатели деятельности с целью проведения контроля, измерения, обобщения практического опыта (постфактумного анализа) в результате событий в системе безопасности, а также с целью непрерывного совершенствования.