Акционерное общество «ПЕТРУС»

(АО «ПЕТРУС»)

УТВЕРЖДЕНА

приказом АО «ПЕТРУС»

от «17» февраля 2026 г. № СБ_2026-19-ПР

ПОЛИТИКА

информационной безопасности акционерного общества «ПЕТРУС»

ИБ-1.0.01-2026

Мытищи
2026

Акционерное общество «ПЕТРУС» - российская производственная компания, специализирующаяся на выпуске и поставке на рынок ПЭТ-преформ, полимерных колпачков и BOPET-плёнок[1] (далее – Общество, Компания).

Компания, учитывая масштабную интеграцию цифровых технологий во все сферы деятельности и по всем бизнес-направлениям, формирует устойчивые механизмы по обеспечению информационной безопасности информационных ресурсов Компании и производственных активов (материальных и нематериальных), финансовых капиталов, всех видов транзакций и передачи информации, проектных работ, защиты персональных данных, включая участие в этих процессах работников Компании, акционеров, инвесторов и контрагентов (деловых партнеров, поставщиков, подрядчиков, клиентов).

Компания осознает характер и уровень вовлеченности своей деятельности в государственную экономику, отраслевой комплекс, федеральные и региональные социально значимые проекты и с максимальной ответственностью подходит к обеспечению устойчивой киберзащищенности информационных активов Компании.

Компания рассматривает защиту информационных ресурсов как один из стратегических приоритетов устойчивого развития и ключевой элемент цифровой трансформации бизнеса и инновационного развития. Система обеспечения информационной безопасности охватывает всю киберсреду Общества по всей цепочке создания стоимости, включая: программное обеспечение, сети и устройства, процессы, информацию, хранящуюся или передаваемую, каналы и способы передачи цифровых данных, непосредственно порядок работы самих пользователей и служб, а также механизмы контроля эффективности управления кибербезопасностью, киберустойчивостью и киберрисками.

Компания следует положениям Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ № 646 от 05.12.2016, определяющей цели, направления и ответственность в области информационной и кибербезопасности, а также признаёт глобальные вызовы, проблемы и тенденции, связанные с аспектами устойчивого развития.

Компания поддерживает инициативы Российской Федерации по обеспечению кибербезопасности в использовании информационно-коммуникационных технологий, относящихся к фундаментальным основам

[1] Далее – Общество, Компания.

информационного общества и необходимости формирования и развития устойчивой глобальной культуры кибербезопасности, отраженные в Указе Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении основ государственной политики Российской Федерации в области международной информационной безопасности».

Компания стремится к совместимости политики информационной безопасности с правом каждого искать, получать и распространять информацию и идеи с учетом того, что такое право может быть ограничено законодательством для защиты интересов национальной и общественной безопасности каждого участника информационного обмена, а также для предотвращения неправомерного использования и несанкционированного вмешательства в информационные ресурсы.

В целях обеспечения надежных и совместимых с передовой практикой процедур по обеспечению и контролю системы информационной безопасности, Компания придерживается Национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 27000-2021 «Системы менеджмента информационной безопасности. Общий обзор и терминология»; ГОСТ Р ИСО/МЭК 27002-2021 «Свод норм и правил применения мер обеспечения информационной безопасности»; ГОСТ Р ИСО/МЭК 27003-2021 Системы менеджмента информационной безопасности. Руководство по реализации»; межгосударственных стандартов: ГОСТ ISO/IEC 27014-2021 «Руководство деятельностью по обеспечению информационной безопасности» ISO/IEC 27701 «Безопасность информационных технологий, кибербезопасность и защита данных», постоянно актуализирует внедрение стандартов ISO в области системы и менеджмента управления киберзащитой в свою практику.

В рамках управления киберрисками Компания придерживается стандартов ISO серии 31000 «Менеджмент рисков» в части управления системой информационной безопасности в ходе реализации проектов, отлаживания бизнес-взаимодействия с котрагентами.

В своей деятельности Компания постоянно оценивает риски бизнес-процессам, влияющие на устойчивость менеджмента производства, и принимает меры к их устранению (уменьшению) за счет:

создания и развития системы управления информационной безопасностью (СУИБ), соответствующей требованиям бизнеса и законодательства Российской Федерации;

прогнозирования, предупреждения, выявления, противодействия и нейтрализации внешних и внутренних угроз информационной безопасности, а также минимизация ущерба от их воздействия;

реализации комплекса мероприятий по обеспечению безопасности персонала и информационных активов;

обеспечения выполнения и контроля соблюдения требований законодательства Российской Федерации и локальных нормативных актов Компании в области информационной безопасности, а также повышения осведомленности персонала в области информационной безопасности.