

Положение о Применимости					
					version 1. 01.12.2020
	#	Идентификация	Включено (I) / Исключено (E)	Статус	Обоснование
5. Политика в области информационной безопасности					
	5.1	Направление управления информационной безопасностью			
	5.1.1	Политики в области информационной безопасности	I	Fully implemented	Часть стандартного способа работы организации
	5.1.2	Обзор политик информационной безопасности	I	Fully implemented	Часть стандартного способа работы организации
6. Организация информационной безопасности					
	6.1	Внутренняя организация			
	6.1.1	Ответственность и роли в области информационной безопасности	I	Fully implemented	Результаты оценки риска
	6.1.2	Разделение обязанностей	I	Fully implemented	Результаты оценки риска
	6.1.3	Контакт с властями	I	Fully implemented	Результаты оценки риска
	6.1.4	Контакт с заинтересованными сторонами	I	Fully implemented	Результаты оценки риска
	6.1.5	Информационная безопасность в управлении проектами	I	Fully implemented	Результаты оценки риска
	6.2	Мобильные устройства и телекоммуникация			
	6.2.1	Политика в отношении мобильных устройств	I	Fully implemented	Результаты оценки риска
	6.2.2	Телекоммуникация	I	Fully implemented	Результаты оценки риска
7. Безопасность HR					
	7.1	До трудоустройства			
	7.1.1	Скрининг	E		Результаты оценки риска
	7.1.2	Условия трудоустройства	I	Fully implemented	Результаты оценки риска
	7.2	Во время работы			
	7.2.1	Ответственность руководства	I	Fully implemented	Часть стандартного способа работы организации
	7.2.2	Осведомленность, образование и профессиональная подготовка в области информационной безопасности	I	Fully implemented	Часть стандартного способа работы организации
	7.2.3	Дисциплинарный процесс	E		Политика управления
	7.3	Увольнение и смена места работы			
	7.3.1	Прекращение или изменение трудовых обязанностей	I	Fully implemented	Часть стандартного способа работы организации
8. Управление активами					
	8.1	Ответственность за активы			
	8.1.1	Инвентаризация активов	I	Fully implemented	Часть стандартного способа работы организации
	8.1.2	Владение активами	I	Fully implemented	Часть стандартного способа работы организации
	8.1.3	Приемлемое использование активов	I	Fully implemented	Часть стандартного способа работы организации
	8.1.4	Возврат активов	I	Fully implemented	Часть стандартного способа работы организации
	8.2	Классификация информации			
	8.2.1	Классификация информации	E		Результаты оценки риска
	8.2.2	Маркировка информации	E		Результаты оценки риска
	8.2.3	Обращение с активами	E		Результаты оценки риска
	8.3	Обработка носителей			
	8.3.1	Управление съемными носителями	I	Fully implemented	Результаты оценки риска
	8.3.2	Утилизация носителей	I	Fully implemented	Результаты оценки риска
	8.3.3	Передача физического носителя	I	Fully implemented	Результаты оценки риска
9. Контроль доступа					
	9.1	Бизнес-требования к контролю доступа			
	9.1.1	Политика контроля доступа	I	Fully implemented	Часть стандартного способа работы организации
	9.1.2	Доступ к сетям и сетевым сервисам	I	Fully implemented	Часть стандартного способа работы организации
	9.2	Управление доступом пользователей			
	9.2.1	Регистрация пользователя и снятие с регистрации	I	Fully implemented	Часть стандартного способа работы организации
	9.2.2	Обеспечение доступа пользователей	I	Fully implemented	Часть стандартного способа работы организации
	9.2.3	Управление привилегированными правами доступа	I	Fully implemented	Часть стандартного способа работы организации
	9.2.4	Управление секретной аутентификационной информацией пользователей	I	Fully implemented	Часть стандартного способа работы организации
	9.2.5	Проверка прав доступа пользователя	I	Fully implemented	Результаты оценки риска
	9.2.6	Удаление или корректировка прав доступа	I	Fully implemented	Результаты оценки риска
	9.3	Обязанности пользователя			
	9.3.1	Использование секретной аутентификационной информации	I	Fully implemented	Часть стандартного способа работы организации
	9.4	Контроль доступа к системе и приложениям			
	9.4.1	Ограничение доступа к информации	I	Fully implemented	Часть стандартного способа работы организации
	9.4.2	Безопасные процедуры входа в систему	I	Fully implemented	Результаты оценки риска
	9.4.3	Система управления паролями	I	Fully implemented	Часть стандартного способа работы организации
	9.4.4	Использование привилегированных служебных программ	I	Fully implemented	Результаты оценки риска
	9.4.5	Контроль доступа к исходному коду программы	I	Fully implemented	Часть стандартного способа работы организации
10. Криптография					
	10.1	Криптографический контроль			
	10.1.1	Политика в отношении использования криптографических средств контроля	I	Fully implemented	Контрактные требования
	10.1.2	Управление ключами	E		
11. Физическая и экологическая безопасность					
	11.1	Безопасные зоны			
	11.1.1	Периметр физической безопасности	I	Fully implemented	Контрактные требования
	11.1.2	Контроль физического входа	I	Fully implemented	Контрактные требования
	11.1.3	Обеспечение безопасности офисов, помещений и сооружений	I	Fully implemented	Контрактные требования
	11.1.4	Защита от внешних и экологических угроз	I	Fully implemented	Контрактные требования

Положение о Применимости					
					version 1. 01.12.2020
	#	Идентификация	Включено (I) / Исключено (E)	Статус	Обоснование
	11.1.5	Работа в безопасных зонах	I	Fully implemented	Контрактные требования
	11.1.6	Зоны доставки и погрузки	I	Fully implemented	Контрактные требования
	11.2	Оборудование			
	11.2.1	Установка оборудования и защита	I	Fully implemented	Контрактные требования
	11.2.2	Вспомогательные утилиты	I	Fully implemented	Контрактные требования
	11.2.3	Безопасность прокладки кабеля	I	Fully implemented	Контрактные требования
	11.2.4	Техническое обслуживание оборудования	I	Fully implemented	Контрактные требования
	11.2.5	Изъятие активов	I	Fully implemented	Контрактные требования
	11.2.6	Безопасность оборудования и активов за пределами помещений	I	Fully implemented	Контрактные требования
	11.2.7	Безопасная утилизация или повторное использование оборудования	I	Fully implemented	Контрактные требования
	11.2.8	Автоматическое пользовательское оборудование	I	Fully implemented	Контрактные требования
	11.2.9	Политика очистки рабочего стола и экрана	I	Fully implemented	Контрактные требования
12. Безопасность операций					
	12.1	Оперативные процедуры и обязанности			
	12.1.1	Документированные операционные процедуры	I	Fully implemented	Часть стандартного способа работы организации
	12.1.2	Управление изменениями	I	Fully implemented	Часть стандартного способа работы организации
	12.1.3	Управление производительностью	I	Fully implemented	Результаты оценки риска
	12.1.4	Разделение сред разработки, тестирования и эксплуатации	I	Fully implemented	Результаты оценки риска
	12.2	Защита от вредоносных программ			
	12.2.1	Средства защиты от вредоносных программ	I	Fully implemented	Часть стандартного способа работы организации
	12.3	Резервная копия			
	12.3.1	Резервное копирование информации	I	Fully implemented	Часть стандартного способа работы организации
	12.4	Ведение журнала и мониторинг			
	12.4.1	Ведение журнала событий	I	Fully implemented	Часть стандартного способа работы организации
	12.4.2	Защита информации журнала	I	Fully implemented	Результаты оценки риска
	12.4.3	Журналы администратора и оператора	I	Fully implemented	Результаты оценки риска
	12.4.4	Синхронизация часов	I	Fully implemented	Результаты оценки риска
	12.5	Управление операционным программным обеспечением			
	12.5.1	Установка программного обеспечения на операционные системы	I	Fully implemented	Результаты оценки риска
	12.6	Управление техническими уязвимостями			
	12.6.1	Управление техническими уязвимостями	I	Fully implemented	Результаты оценки риска
	12.6.2	Ограничения на установку программного обеспечения	I	Fully implemented	Результаты оценки риска
	12.7	Обзор аудита информационной системы			
	12.7.1	Средства контроля аудита информационных систем	I	Fully implemented	Результаты оценки риска
13. Безопасность связи					
	13.1	Управление сетевой безопасностью			
	13.1.1	Сетевые элементы управления	I	Fully implemented	Результаты оценки риска
	13.1.2	Безопасность сетевых служб	I	Fully implemented	Результаты оценки риска
	13.1.3	Сегрегация в сетях	E	Fully implemented	Результаты оценки риска
	13.2	Передача информации			
	13.2.1	Политика и процедуры передачи информации	I	Fully implemented	Результаты оценки риска
	13.2.2	Соглашения о передаче информации	I	Fully implemented	Результаты оценки риска
	13.2.3	Электронные сообщения	I	Fully implemented	Результаты оценки риска
	13.2.4	Соглашения о конфиденциальности или неразглашении	I	Fully implemented	Контрактные требования
14. Слияния, разработка и техническое обслуживание					
	14.1	Требования к безопасности информационных систем			
	14.1.1	Анализ и спецификации требований безопасности	I	Fully implemented	Часть стандартного способа работы организации
	14.1.2	Защита служб приложений в общедоступных сетях	I	in progress	Результаты оценки риска
	14.1.3	Защита транзакций служб приложений	I	in progress	Результаты оценки риска
	14.2	Безопасность в процессах разработки и поддержки			
	14.2.1	Политика безопасного развития	E		Не применимо к организации
	14.2.2	Процедуры контроля системных изменений	E		Не применимо к организации
	14.2.3	Технический обзор приложений после изменения операционной платформы	E		Не применимо к организации
	14.2.4	Ограничения на внесение изменений в пакеты программного обеспечения	E		Не применимо к организации
	14.2.5	Принципы проектирования безопасных систем	E		Не применимо к организации
	14.2.6	Безопасная среда разработки	E		Не применимо к организации
	14.2.7	Аутсорсинговая разработка	E		Не применимо к организации
	14.2.8	Тестирование безопасности системы	E		Не применимо к организации
	14.2.9	Приемочное тестирование системы	E		Не применимо к организации
	14.3	Тестовые данные			
	14.3.1	Защита тестовых данных	E		Не применимо к организации
15. Отношения с поставщиками					
	15.1	Информационная безопасность в отношениях с поставщиками			
	15.1.1	Политика информационной безопасности в отношениях с поставщиками	I	Fully implemented	Часть стандартного способа работы организации
	15.1.2	Обеспечение безопасности в рамках соглашений с поставщиками	I	Fully implemented	Часть стандартного способа работы организации
	15.1.3	Цепочка поставок информационно-коммуникационных технологий	I	Fully implemented	Часть стандартного способа работы организации
	15.2	Управление поставщиками услуг			

Положение о Применимости

version 1. 01.12.2020

	#	Идентификация	Включено (I) / Исключено (E)	Статус	Обоснование
	15.2.1	Мониторинг и анализ услуг поставщиков	I	not yet started	Результаты оценки риска
	15.2.2	Управление изменениями в услугах поставщика	I	Fully implemented	Результаты оценки риска
16. Управление инцидентами информационной безопасности					
	16.1	Управление инцидентами информационной безопасности и улучшения			
	16.1.1	Обязанности и процедуры	I	Fully implemented	Контрактные требования
	16.1.2	Отчетность о событиях информационной безопасности	I	Fully implemented	Контрактные требования
	16.1.3	Отчетность о слабых сторонах информационной безопасности	I	Fully implemented	Контрактные требования
	16.1.4	Оценка событий информационной безопасности и принятие решений по ним	I	Fully implemented	Контрактные требования
	16.1.5	Реагирование на инциденты информационной безопасности	I	Fully implemented	Контрактные требования
	16.1.6	Извлечение уроков из инцидентов информационной безопасности	I	Fully implemented	Контрактные требования
	16.1.7	Сбор доказательств	I	Fully implemented	Контрактные требования
17. Аспекты ИБ в управлении непрерывностью бизнеса					
	17.1	Непрерывность информационной безопасности			
	17.1.1	Планирование непрерывности информационной безопасности	E		В силу характера организации, принято управленческое решение не внедрять
	17.1.2	Обеспечение непрерывности информационной безопасности	E		В силу характера организации, принято управленческое решение не внедрять
	17.1.3	Проверка, обзор и оценка непрерывности информационной безопасности	E		В силу характера организации, принято управленческое решение не внедрять
	17.1	Избыточности			
	17.1.4	Наличие средств обработки информации	E		В силу характера организации, принято управленческое решение не внедрять
18. Соответствие					
	18.1	Соблюдение юридических и договорных требований			
	18.1.1	Определение применимого законодательства и договорных требований	I	Fully implemented	Правовые предписания
	18.1.2	Права интеллектуальной собственности	I	Fully implemented	Правовые предписания
	18.1.3	Защита записей	I	Fully implemented	Часть стандартного способа работы организации
	18.1.4	Конфиденциальность и защита личной информации, позволяющей установить личность	I	Fully implemented	Правовые предписания
	18.1.5	Регулирование криптографического контроля	I	Fully implemented	Правовые предписания
	18.2	Обзоры информационной безопасности			
	18.2.1	Независимый обзор информационной безопасности	I	Fully implemented	Часть стандартного способа работы организации
	18.2.2	Соответствие политикам и стандартам безопасности	I	Fully implemented	Часть стандартного способа работы организации
	18.2.3	Проверка технического соответствия	I	Fully implemented	Результаты оценки риска