УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2018 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ДОЛЖНОСТЬ РАБОТНИКА	Должность относится к категории специалистов. Назначение на должность и освобождение от нее осуществляется приказом Генерального директора Компании
1.2. СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ	Департамент по безопасности
1.3. ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ	Директор по информационной безопасности
1.4. КЕМ ЗАМЕЩАЕТСЯ	Директором по информационной безопасности
1.5. КОГО ЗАМЕЩАЕТ	Директора по информационной безопасности
1.6. РУКОВОДСТВУЕТСЯ	Действующим трудовым законодательством и иными нормативными актами Российской Федерации, внутренними нормативными актами Компании, а также настоящей должностной инструкцией.
1.7. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ	
1.7.1. Высшее образование в сфере обеспечения безопасности, информационных технологий, защиты информации.	
1.7.2. Опыт работы в бизнес-структурах на должностях, связанных с обеспечением защиты информации от 1 года.	
1.7.3. Образование, дополнительная профессиональная подготовка, знания, навыки, опыт и т.п., необходимые для осуществления должностных обязанностей, указанных в разделе 3, в том числе базовые знания по следующим разделам: - повышение квалификации в сфере экономической безопасности; - личные качества: ответственность, коммуникабельность; - развитые аналитически способности; - знание принципов организации обеспечения безопасности объектов предприятия, его персонала и информации, являющейся коммерческой тайной и информации относящейся к персональным данным; тактики защиты объектов, информации, персонала предприятия от преступных посягательств;	
1.7.4. Уверенное практическое владение компьютером (Microsoft Office – Outlook, Excel, Word, PowerPoint и др.).	

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

2.1.1 Выполнять работу в области защиты персональных данных (ПДн) Компании:

- разрабатывать требования для подразделений Компании по выполнению законодательства РФ в области защиты ПДн;
- контролировать выполнение требований по защите ПДн в Компании;
- разрабатывать нормативно-методические документы в сфере защиты ПДн в Компании;
- проводить расследования по фактам нарушения норм защиты ПДн в Компании;
- консультировать подразделения и сотрудников Компании по вопросам защиты ПДн;
- информировать Руководство о состоянии защиты ПДн в Компании, о нарушениях норм защиты ПДн, о результатах соответствующих проверок и расследований;
- разрабатывать предложения по совершенствованию защиты ПДн в Компании;
- разрабатывать предложения по формированию сметы затрат, необходимых для решения задач обеспечения защиты ПДн в Компании.

2.1.2 Подготавливать нормативные правовые документы по линии обеспечения информационной безопасности в Компании, заключений и предложений по проектам локальных нормативных актов Компании.
2.1.3 Выполнять работы по повышению осведомленности сотрудников Компании в вопросах обеспечения информационной безопасности.
2.1.4 Разрабатывать материалы для самостоятельного изучения сотрудниками Компании.
2.1.5 Проводить анализ опыта деятельности по обеспечению информационной безопасности и осуществлять его внедрение в интересах Компании.
2.1.6 Участвовать в создании и внедрении единых форм и методов в деятельности подразделений безопасности Компании.
2.1.7 Проводить проверочные мероприятия в области обеспечения защиты конфиденциальной информации в структурных подразделениях Компании.
2.1.8 Выявлять бизнес-процессы Компании, в ходе которых возникают угрозы информационным ресурсам и требующие принятия дополнительных мер по обеспечению информационной безопасности.
2.1.9 Вырабатывать единые требования (цели, задачи, методы и средства работы) по обеспечению информационной безопасности Компании.
2.1.10 Эксплуатировать технические средства защиты информации.
2.1.11 Организовывать работы по профилактике и контролю инцидентов информационной безопасности в Компании (в том числе предупреждать незаконный доступ к информационным ресурсам и утечки конфиденциальной информации).
2.1.12 Сопровождать деятельность Компании в сфере информационных технологий, участвовать в проектах по внедрению информационных систем в части контроля соответствия требованиям нормативных правовых документов РФ и Компании по вопросам обеспечения информационной безопасности.
2.1.13 Организовывать планирование и отчетную работу в интересах обеспечения информационной безопасности Компании, согласовывать планы работы подразделений информационной безопасности Компании, осуществлять контроль их подготовки и выполнения.
2.1.14 Получать, обобщать и анализировать результаты, принимаемых в Компании мер в области информационной безопасности, прогнозировать развитие событий в информационной сфере, подготавливать заключения и рекомендации.
2.1.15 Осуществлять методическую помощь подразделениям информационной безопасности Компании при подготовке распорядительных и нормативных документов по линии обеспечения информационной безопасности.

3. ИМЕЕТ ПРАВО

3.1.1 Запрашивать документы, материалы и другую информацию, необходимую для исполнения должностных обязанностей.
3.1.2 Принимать участие в обсуждении вопросов, касающихся деятельности своего структурного подразделения.
3.1.3 Участвовать в мероприятиях Компании в рамках своей компетенции.
3.1.4 Вести деловую переписку и представлять интересы Компании в пределах своей компетенции.
3.1.5 Подписывать и визировать документы, в пределах своей компетенции (для лиц, имеющих право подписывать и визировать документы).
3.1.6 Вносить предложения по оптимизации работы своего структурного подразделения и всего Компании.

3.1.7 Быть обеспеченным необходимыми техническими и программными средствами для выполнения в срок поставленных задач.

4. НЕСЕТ ОТВЕТСТВЕННОСТЬ

4.1.1 За невыполнение указаний и поручений руководства Компании, указаний непосредственного Руководителя, плана работ и несоблюдение условий труда Работников, находящихся в подчинении.

4.1.2 За нечеткое и несвоевременное выполнение своих должностных обязанностей, предусмотренных настоящей инструкцией.

4.1.3 За сохранность находящегося в использовании имущества.

4.1.4 За несоблюдение трудовой дисциплины, Правил внутреннего трудового распорядка, иных локальных нормативных актов Компании.

4.1.5 За ненадлежащее или несанкционированное использование, раскрытие, разглашение, распространение, передачу или комментирование конфиденциальной информации (включая ИКТ и инсайдерскую информацию) о Компании, дивизионы, их сотрудниках или контрагентах (в т. ч. за совершение сделок с ценными бумагами на основании такой информации), утрату документов, содержащих такую информацию, нарушение установленных правил обращения с ней, сбор сведений, составляющих конфиденциальную информацию, если это не является необходимым для надлежащего осуществления своих должностных обязанностей, незаконное получение денег, ценных бумаг, услуг, иного имущества, а равно незаконное пользование услугами имущественного характера, за совершение неправомерных или неэтичных действий (бездействия) в связи с занимаемым служебным положением, неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для персональных компьютеров, нарушение правил эксплуатации персональных компьютеров или их сети и другие типы нарушений.

5 РЕКВИЗИТЫ СТОРОН

РАЗРАБОТАЛ:			
	Ведущий специалист по информационной безопасности и защите персональных данных	_____ (подпись)	
СОГЛАСОВАНО:			
	Заместитель Генерального директора по безопасности	_____ (подпись)	

		_____ (подпись)	

ЛИСТ ОЗНАКОМЛЕНИЯ

С должностной инструкцией ознакомлен(а) и обязуюсь выполнять свои обязанности согласно должностной инструкции. Один экземпляр должностной инструкции мною получен:

№ п/п	ФИО	Подпись	Дата