KCELL SECURITY DIRECTIVES	**ДИРЕКТИВЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АО «КСЕЛЛ»**
1 Description This document (the "Security Directives") describes the security requirements applicable to Suppliers (as defined below) and other identified business partners to the Kcell JSC. Additional security requirements may apply in particular cases if agreed by involved parties.	**1 Описание** Настоящий документ ("Директивы по обеспечению безопасности") описывает требования по безопасности, применимые к Поставщикам (согласно определению ниже), а также определенным деловым партнерам АО "Кселл". Дополнительные требования по безопасности могут применяться в отдельных случаях при наличии согласия вовлеченных сторон.
2 Definitions 1. **"Agreement"** shall mean the agreement between Kcell JSC and Supplier or other identified business partner to the Kcell JSC under which the Security Directives apply, and to which the Security Directives are part thereof. 2. **"Kcell's Data"** shall mean data or other information that the Kcell, or a person acting on behalf of the Kcell, makes available to the Supplier, and the result of Supplier's processing of such data. 3. **"Information Processing Facilities"** shall mean any information processing system, services or infrastructure, or the physical locations housing them. 4. **"Log"** shall mean to record details of information or events in an organized record-keeping system, usually sequenced in the order in which the information or events occurred. 5. **"Personal Data"** shall, subject to local, applicable mandatory law. 6. **"Services"** shall mean the services to be provided by the Supplier to the Kcell, or a person acting on behalf of the Supplier as further defined in the Agreement between the parties. 7. **"Supplier"** shall refer to the counter-party who supplies any kind of deliverables to Kcell identified as "Supplier", "Vendor, "Partner" or the equivalent in the relevant Agreement. 8. **"Supplier Personnel"** shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers. 9. **"Security Control"** shall mean a technical countermeasure, an organizational setup or a process, that helps to maintain IT systems security-quality properties. 10. **"Security Incident"** shall mean a single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening security. **11. "Sensitive Products"** and **"Sensitive Services"** shall mean any product or Services defined as sensitive by the Kcell. Sensitive Products or Sensitive Services shall be clearly documented in the applicable Agreement.	**2 Определения** 1. **"Соглашение"** означает соглашение между АО "Кселл" и Поставщиком или другим установленным бизнес-партнером АО "Кселл", в соответствии с которым применяются Директивы по безопасности и частью которого они являются. 2. **"Данные Kcell"** означает данные или другую информацию, которую Kcell, или лицо, действующее от имени Kcell, предоставляет поставщику, а также результат обработки таких данных Поставщиком. 3. **"Средства обработки информации"** означает любые системы, услуги или инфраструктуру по обработке информации, или физические помещения, которых они размещаются. 4. **"Вести учет"** означает записывать детали информации или события в системе учета; как правило, в той последовательности, в которой возникает такая информация или событие. 5. **"Персональные данные"**, с учетом применимого обязательного законодательства Республики Казахстан. 6. **"Услуги"** означает услуги, оказываемые Поставщиком компании Kcell, или лицом, действующим от имени Поставщика, в соответствии с определением, приведенным в Соглашении между сторонами. 7. **"Поставщик"** означает контрагент, осуществляющий поставки компании Kcell; также именуется "Продавец", "Партнером" или имеет иное эквивалентное название, определенное соответствующим Соглашением. 8. **"Персонал Поставщика"** означает любое лицо, работающее от имени Поставщика (работники, консультанты, субподрядчики и т.д.). 9. **"Контроль безопасности**" означает технические меры противодействия, организационную структуру или процесс, позволяющий поддерживать необходимые технические и качественные параметры безопасности IT-систем. 10. **"Инцидент информационной безопасности"** означает единичное или серию нежелательных или неожиданных событий безопасности, создающих высокую вероятность ухудшения экономической деятельности организации и угрозы ее безопасности. **11. "Стратегические товары"** и **"Стратегические услуги"** означает любой продукт или Услуги, определенные компанией Kcell как стратегические. Стратегические

	товары/услуги должны быть четко указаны в соответствующем Соглашении.
3 Scope The Security Directives apply when: 1. The Supplier will process Kcell's Data. 2. The Supplier will access Kcell's premises. 3. The Supplier will access Kcell's network or IT systems including remote access. 4. The Supplier will handle Kcell's information processing equipment. 5. The Kcell has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services and identified Supplier as such under the relevant Agreement.	**3 Область применения** Директивы по обеспечению безопасности применяются при: 1. обработке Поставщиком данных Kcell; 2. нахождении Поставщика на территории Kcell; 3. предоставлении Поставщику доступа к сетям и IT-системам Kcell, в том числе через удаленный доступ; 4. использовании Поставщиком оборудования обработки информации Kcell; **5.** при привлечении Поставщика компанией Kcell в качестве провайдера Стратегических товаров и/или Стратегических услуг на основании соответствующего договора.
4 The Supplier´s overall responsibility 1. The Supplier is fully responsible for the Supplier Personnel's compliance with the Security Directives. 2. The Supplier shall implement the measures required to ensure compliance to the Security Directives prior to commencing any assignment for the Kcell. 3. The Supplier shall, at the request of the Kcell, inform the Kcell how the Supplier complies with the Security Directives and what measures the Supplier has taken to comply with the Security Directives. 4. The Supplier shall inform the Kcell at speakup@kcell.kz about any Security Incident (including but not limited to incidents in relation to the processing of Personal Data) as soon as possible but no later than within 24 hours after the Security Incident has been identified. See incident management bellow. 5. The Supplier shall guarantee that any processing of Kcell's Data will be compliant with the Security Directives. 6. The Supplier shall return or destroy (as determined by the Kcell) any Kcell's Data and the copies thereof. The Supplier shall confirm in writing to the Kcell that the Supplier has met this requirement on termination of the Agreement or at the request of the Kcell. **7.** The Supplier shall not allow any access to Kcell's Data (it may also concern new, extended, updated, prolonged or in any other way changed real-time network access) in breach of the Agreement to any party without prior written approval by the Kcell.	**4.Полная ответственность поставщика** 1. Поставщик несет полную ответственность за соблюдение персоналом Поставщика Директив по обеспечению безопасности. 2. Поставщик обязан осуществить меры, необходимые для обеспечения соответствия Директивам по безопасности перед началом выполнения любого задания для Kcell. 3. По требованию Kcell, Поставщик обязан информировать Kcell о том, как обеспечивается соблюдение Директив по безопасности и какие меры были приняты Поставщиком для обеспечения соответствия требованиям Директив по безопасности. 4. Поставщик обязан уведомлять Kcell по электронному адресу speakup@kcell.kz о любых Инцидентах безопасности (включая, но не ограничиваясь, инциденты, связанные с обработкой Персональных данных) в кратчайшие сроки, но не позднее, чем в течение 24 часов после обнаружения Инцидента безопасности. См. информацию по управлению инцидентами ниже. 5. Поставщик гарантирует, что любая обработка Данных Kcell будет осуществлять в строгом соответствии с Директивами по безопасности. 6. Поставщик обязан вернуть или уничтожить (на усмотрение Kcell) любые Данные Kcell и их копии. Поставщик обязан представить Kcell письменное подтверждение исполнения данного требования в случае прекращении Соглашения или по требованию Kcell. **7.** Поставщик не должен предоставлять третьим лицам доступ к Данным Kcell (в том числе новый, расширенный, обновленный, продолжительный или иной формы доступ к сети в режиме реального времени) в нарушение Соглашения без предварительного письменного одобрения со стороны Kcell.
5. Security Requirements **5.1 Risk management** 1. The Supplier shall identify security risks and take necessary actions to control and mitigate such risks. 2. The Supplier shall have documented processes and routines for handling risks within its operations. 3. The Supplier shall periodically assess the risks related to	**5. Требования безопасности** **5.1 Управление рисками** 1. Поставщик обязан выявлять риски в области безопасности и принимать необходимые меры для контроля и снижения таких рисков. 2. Поставщик обязан иметь документально оформленные процессы и процедуры по обработке рисков в рамках

information systems and processing, storing and transmitting information.	своей деятельности. 3. Поставщик должен периодически проводить оценку рисков, связанных с информационными системами и обработкой, хранением и передачей информации.
5.2 Information security policies 1. The Supplier shall have a defined and documented information security management system (ISMS) including an information security policy and procedures in place, which shall be approved by the Supplier's management. They shall be published within Supplier´s organization and communicated to relevant Supplier Personnel. 2. The Supplier shall periodically review the Supplier's security policies and procedures and update them if required to ensure their compliance with the Security Directives.	**5.2 Политики в области информационной безопасности** 1. Поставщик должен иметь разработанную и документально оформленную систему управления информационной безопасностью (СУИБ), в том числе действующую политику и процедуры по обеспечению информационной безопасности, утвержденные руководством Поставщика. Такие документы должны быть опубликованы на внутренних ресурсах Поставщика и доведены до сведения соответствующего Персонала Поставщика. 2. Поставщик должен периодически пересматривать политику и процедуры в области безопасности и обновлять их в случае необходимости в целях обеспечения их соответствия Директивам безопасности.
5.3 Organization of information security 1. The Supplier shall have defined and documented security roles and responsibilities within its organization. 2. The Supplier shall appoint at least one person who has appropriate security competence and who has an overall responsibility for implementing the security measures under the Security Directives and who will be the contact person for Kcell's security staff.	**5.3 Организация информационной безопасности** 1. Поставщик должен определить и документально закрепить роли и обязанности по обеспечению безопасности в рамках своей организации. 2. Поставщик должен назначить, по меньшей мере, одного человека, обладающего надлежащей компетенцией в области безопасности, который будет нести общую ответственность за осуществление мер безопасности в соответствии с Директивами по безопасности и являться контактным лицом для сотрудников службы безопасности Kcell.
5.4 Human resource security 1. The Supplier shall ensure that the Supplier Personnel handles information in accordance with the level of confidentiality required under the Agreement. 2. The Supplier shall ensure that relevant Supplier Personnel is aware of the approved use (including use restrictions as the case may be) of information, facilities and systems under the Agreement. Kcell has the right to request a signed receipt from each and every Supplier Personnel stating that he or she has understood and will comply with the Security Directives and the approved use of information, systems and facilities. 3. The Supplier shall ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy, meets established security criteria and has been subject to appropriate screening and background verification. 4. The Supplier shall provide Kcell in advance with a list of all the Supplier's employees, consultants, contractors and other individuals working under the Supplier's responsibility who are performing services under the agreement, containing name, personal identity number and contact information such as telephone number and e-mail address ("the Supplier's Personnel List") and shall keep such list updated at all times during the period of the	**5.4 Обеспечение безопасности персонала** 1. Поставщик должен обеспечить, что Персонал Поставщик осуществляет обработку информации в соответствии с уровнем конфиденциальности, установленной в Соглашении. 2. Поставщик должен обеспечить осведомленность своего Персонала о разрешенном использовании (в том числе, в зависимости от обстоятельств, ограничении в использовании) информации, средств и систем в соответствии с Соглашением. Kcell вправе потребовать предоставления соответствующей расписки от каждого работника Поставщика в том, что они ознакомлены, понимают и обязуются соблюдать Директивы по безопасности и использовать информацию, средства и системы только в разрешенных целях. 3. Поставщик должен гарантировать, что любой его работник, привлеченный к выполнению задания по Соглашению, является надежным, отвечает установленным критериям безопасности и прошел соответствующий скрининг и проверку личных данных. 4. Поставщик должен заранее предоставить Kcell список всех сотрудников, консультантов, подрядчиков и других лиц Поставщика, работающих под ответственность Поставщика, предоставляющих услуги по договору. Список должен содержать имя, личный код и

agreement in question. The Supplier's Personnel List may at any point in time be used by Kcell in audit situations as reference to verify the validity of issued access rights towards Kcell's IT-systems or premises.

5. The Supplier shall ensure that Supplier Personnel with security responsibilities is adequately trained to carry out security related duties.
6. The Supplier shall provide or ensure periodical security awareness training to relevant Supplier Personnel. Such Supplier training shall include, without limitation:
   a. How to handle customer information security (i.e. the protection of the confidentiality, integrity and availability of information);
   b. Why information security is needed to protect customers information and systems;
   c. The common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);
   d. The importance of complying with information security policies and applying associated standards/procedures;
   e. Personal responsibility for information security (such as protecting customer's privacy-related information and reporting actual and suspected Security Incidents).
7. The Supplier shall ensure that the Supplier's Personnel performing tasks for Kcell are aware of the confidentiality obligations for telecommunication data and business information related to the assignment, as well as the approved use of information, facilities and systems. The Kcell has the right to request signed receipt from the Supplier's Personnel stating that the individual has understood and will comply with the obligations, accepted use of systems and facilities.

5.5 Asset management

1. The Supplier shall have a defined and documented asset management system in place, and maintain up-to-date records of all relevant assets and their owners. Information assets include but are not limited to IT systems, backup and/or removable media containing sensitive information, access rights, software and configuration.
2. The Supplier shall label, treat and protect information according to a pre-defined information classification system in accordance with valid security standards at that time (including removable media storage, disposal and physical transfer).

контактную информацию, такую как номер телефона и адрес электронной почты ("Список Персонала Поставщика"), и Поставщик должен вносить в список изменения в любое время в течение срока действия договора. Список Персонала Поставщика может в любой момент времени быть использован Kcell при осуществлении проверок в качестве ссылки для проверки действительности предоставленных прав доступа к IT-системам или помещениям Kcell.

5. Поставщик должен обеспечить прохождение Персоналом Поставщика, отвечающего за безопасность, необходимого обучения для надлежащего осуществления своих обязанностей по обеспечению безопасности.
6. Поставщик должен обеспечить проведение регулярного обучения по безопасности для соответствующего Персонала поставщика. Такое обучение должно включать в себя, без ограничения, следующее:
   a. Как обеспечить информационную безопасность клиента (т.е. защита конфиденциальности, целостности и доступности информации);
   b. Почему необходима информационная безопасность для защиты информации и систем клиентов;
   c. Общие типы угроз безопасности (например, кража личных данных, вредоносные программы, хакеры, утечка информации и внутренняя угроза);
   d. Важность соблюдения политики информационной безопасности и применения соответствующих стандартов/процедур;
   e. Персональная ответственность за информационную безопасность (например, защита личных данных клиента, а также информирование о фактических и предполагаемых случаях нарушения безопасности).
7. Поставщик должен обеспечить осведомлённость Персонала Поставщика, выполняющего задания для Kcell, об обязательствах по соблюдению конфиденциальности телекоммуникационных данных и бизнес-информации, связанных с заданием, а также об утверждённом использовании информации, средств и систем. Kcell вправе потребовать расписку от Персонала Поставщика в том, что все работники понимают и обязуются соблюдать обязательства по использованию систем и средств в разрешенных целях.

5.5 Управление активами

1. Поставщик должен иметь документально оформленную и действующую систему управления активами, и вести своевременный учет всех соответствующих активов и их владельцев. Информационные активы включают в себя, но не ограничиваются ими, IT-системы, резервное копирование и / или съемные носители, содержащие конфиденциальную информацию, права доступа, программное обеспечение и конфигурациион.
2. Поставщик обязан маркировать, обращаться и обеспечивать защиту информации в соответствии с заранее определенной системой классификации

	информации в соответствии с действующими в данный момент времени стандартами безопасности (включая хранение, утилизацию и физическую передачу сменные носителей информации).
5.6 Access control 1. The Supplier shall have a defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for the Supplier Personnel in place. 2. The supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights. 3. The Supplier shall assign all access privileges based on the principle of need-to-know and principle of least privilege. 4. The Supplier shall use strong authentication (2-factor) for system administrators or other high privilege users, including remote access users, when working with systems that contain Kcell's Data. 5. The Supplier shall ensure that the Supplier Personnel has a personal and unique identifier (user ID), and use an appropriate authentication technique, which confirms and ensures the identity of users. 6. The Supplier shall inform Kcell without undue delay about changes in the Supplier's Personnel having access to Kcell information.	**5.6 Управление доступом** 1. Поставщик должен иметь документально оформленную и действующую политику по управлению доступом на объекты, сайты, в сети, системы, приложения и к информации/данным (включая управление физическим, логическим и удаленным доступом), процесс авторизации для предоставления пользовательского доступа и привилегий, процедуры по отмене права доступа и приемлемое использование привилегий доступа Персоналом Поставщика. 2. Поставщик должен иметь документально оформленную и действующую процедуру по регистрации/отмене регистрации пользователей для предоставления прав доступа. 3. Поставщик должен назначить все привилегии доступа, исходя из принципа служебной необходимости и принципа наименьших привилегий. 4. Поставщик должен использовать строгую (2-факторную) систему идентификации для системных администраторов или других пользователей, обладающих высокими привилегиями, в том числе пользователей удаленного доступа, при работе с системами, содержащими Данные Kcell. 5. Поставщик должен гарантировать, что Персонал Поставщика имеет личный и уникальный идентификатор (user ID), и использует соответствующий способ аутентификации для подтверждения и гарантии подлинности пользователей. 6. Поставщик обязан без неоправданных задержек информировать Kcell об изменениях в Персонале Поставщика, имеющего доступ к информации Kcell.
5.7 Cryptography 1. The Supplier shall ensure proper and effective use of cryptography on information classified as confidential and secret (such as Personal Data) in accordance with the Kcell's confidentiality classification scheme as further detailed below. 2. The Supplier shall protect cryptographic keys.	**5.7 Криптография** 1. Поставщик должен обеспечить надлежащее и эффективное применение криптографии к информации, отнесенной к конфиденциальной и тайной (например, Персональные данные) в соответствии со схемой классификации конфиденциальности информации Kcell как подробно изложено ниже. 2. Поставщик должен обеспечить защиту криптографических ключей.
5.8 Physical and environmental security 1. The Supplier shall protect Information Processing Facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection. 2. The Supplier shall protect goods received or sent on behalf of the Kcell from theft, manipulation and destruction.	**5.8 Личная безопасность и безопасность окружающей среды** 1. Поставщик должен обеспечить защиту Средств обработки информации от внешних и экологических угроз и опасностей, включая перебои электроснабжения / неполадки в электропроводке и другие нарушения, вызванных отказами энергетических систем. Сюда относится физический периметр и защита доступа. 2. Поставщик должен защищать товары, полученные или отправленные от имени Kcell, от кражи, махинаций и

5.8.1 Admission to Kcell's premises and Kcell's leased premises

The Supplier's admission to Kcell's premises and property (such as datacentre buildings, office buildings, technical sites) is subject to the following:

1. The Supplier shall follow local regulations (such as regulations for "restricted areas") for Kcell's premises when performing the assignments under the Agreement.
2. Supplier Personnel shall carry ID card or a visitor's badge visible at all time when working within the Kcell's premises.
3. After completing the assignment, or when Supplier Personnel is transferred to other tasks, the Supplier shall without delay inform the Kcell of the change and return any keys, key cards, certificates, visitor's badges and similar items.
4. Keys or key cards shall be personally signed for by Supplier Personnel and shall be handled according to the written rules given upon receipt.
5. Loss of the Kcell's key or key card shall be reported without delay to the Kcell.
6. Photographing in or at the Kcell's premises without permission is prohibited.
7. Kcell's goods shall not be removed from Kcell's premises without permission.
8. Supplier Personnel shall not allow unauthorized persons access to the premises.
9. In the event of Supplier personnel's non-compliance with the agreement, Kcell is entitled to deny, with immediate effect, the access to Kcell's premises and to request all keys, key cards, etc., handed out to be returned without undue delay.

5.8.2 General rules concerning Kcell's premises

Supplier's Personnel shall adhere to the following general rules regarding Kcell's premises

1. Smoking is prohibited on Kcell's premises, with the exception of dedicated smoking areas.
2. Consumption of alcohol or drugs (other than prescribed pharmaceutical drugs) on Kcell's premises is prohibited.
3. Spending the night on Kcell's premises or parking caravans or similar vehicles on Kcell's property is prohibited without previous consent.
4. No space in Kcell's premises may be used by staff as storage rooms, unless otherwise agreed.
5. The use of computers, telephones, printers, fax machines or

разрушения.

5.8.1 Допуск к помещениям Kcell и помещениям, арендованным Kcell

Допуск Поставщика на территорию и к имуществу Kcell (здания центра обработки данных, офисные здания, технически сайты) должно осуществляться с соблюдением следующих правил:

1. При выполнении задания в соответствии с Соглашением, Поставщик обязуется соблюдать требования национального законодательства (например, законодательства в области зон ограниченного доступа).
2. При работе в помещениях Kcell, Персонал Поставщика обязан иметь при себе и постоянно носить удостоверение личности или пропуск посетителя на видном месте.
3. По окончании выполнения задания, или в случае направления Персонала Поставщика на решение других задач, Поставщик обязан незамедлительно уведомить Kcell о таком изменении и вернуть или изменить распределение ключей, магнитных ключей, удостоверений, пропусков посетителей и других средств идентификации.
4. Ключи или магнитные ключи должны быть оформлены индивидуально для определенного сотрудника из числа Персонала Поставщика, и ключи или магнитные ключи должны использоваться в соответствии с письменными правилами, приведёнными на расписке в получении.
5. Информация об утере ключа или магнитного ключа Kcell незамедлительно доводится до сведения Kcell.
6. Фотосъемка на территории и объектах Kcell без соответствующего разрешения запрещена.
7. Запрещено без соответствующего разрешения выносить товары, принадлежащие Kcell, с его территории.
8. Персоналу Поставщика запрещается предоставлять посторонним лицам доступ на территорию Kcell.
9. В случае неисполнения Персоналом Поставщика условий Соглашения, Kcell вправе незамедлительно отказать Поставщику в предоставлении на свою территорию и потребовать возврата ключей, ключей-карт и т.д., предоставленных с условием возврата без необоснованной задержки по требованию/

5.8.2. Общие правила, касающиеся помещений Kcell

Персонал Поставщика должен придерживаться следующих общих правил, касающихся помещений Kcell:

1. Курение в помещениях Kcell запрещено, за исключением выделенных мест для курения.
2. Запрещено потребление алкоголя или наркотиков (кроме предписанных фармацевтических препаратов) в помещениях Kcell.
3. Ночёвка в помещениях Kcell или на стоянках жилых прицепов или аналогичных транспортных средств на территории Kcell запрещается без получения предварительного согласия.
4. Ни одна из зон на территории Kcell не может быть

any other equipment owned by Kcell is prohibited other than to the extent of the agreement otherwise agreed.

6. Property of Kcell shall not be removed from Kcell premises without permission.
7. Photographing in Kcell's premises is prohibited without permission.
8. If the work the Supplier is going to perform involves risk for dust, noise, vibrations or fire, the Supplier shall obtain Kcell's permission for such action(s) in advance.
9. Alarms such as such fire alarm, burglar alarm and distress alarm are only to be disabled after permission from Kcell. Restoration of alarm system shall be done without undue delay after work has been completed. Procedures and responsibilities before, during and after the disabling of the alarm are to be specified in the agreement and conform to local laws and regulations.
10. The Supplier is responsible for keeping windows and doors locked within the work area and that no unauthorized persons can access the premises.
11. The Supplier's Personnel shall keep their working places neat and tidy. Litter and packaging material shall be promptly removed and discarded at a location specified by Kcell.
12. Emergency equipment or fire escape routes shall not be blocked as a result of Supplier activities.
13. Supplier shall give its personnel safety training before they start working in the Kcell's premises.

5.9 Operations security

1. The Supplier shall have an established change management system in place for making changes to business processes, Information Processing Facilities and systems. The change management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, roll back procedures to recover from failed changes, logs that show, what has been changed, when and by whom.
2. The Supplier shall implement malware protection to ensure that any software used for Supplier's provision of the deliverables to the Kcell is protected from malware.
3. The Supplier shall make backup copies of critical information and test back-up copies to ensure that the information can be restored as agreed with the Kcell.
4. The Supplier shall Log and monitor user's activities,

использована сотрудниками в качестве складских помещений, если сторонами не установлено иное.

5. Запрещено использование компьютеров, телефонов, принтеров, факсов или любого другого оборудования, принадлежащего Kcell, за исключением случаев, когда в договоре предусмотрено иное.
6. Собственность Kcell не может быть удалена из помещения Kcell без разрешения.
7. Фотографирование в помещениях Kcell без разрешения запрещено.
8. Если при производстве работ, которые Поставщик должен выполнить, есть опасность запыления, возникновения шума, вибрации или пожара, Поставщик обязан заранее получить разрешение Kcell для осуществления таких работ.
9. Сигнализация, такая как пожарная сигнализация, охранная сигнализация и система оповещения о бедствии, может быть отключена только с разрешения Kcell. Система охранной сигнализации должна быть незамедлительно восстановлена после завершения работ. Процедуры и действия, осуществляемые до, во время и после отключения сигнализации, должны быть указаны в договоре и в соответствии с местными законами и правилами.
10. Поставщик несёт ответственность за то, что окна и двери в рабочей зоне будут находиться в закрытом состоянии, а также обеспечить невозможность получения доступ в помещения посторонним лицам.
11. Персонал поставщика должен содержать свои рабочие места в чистоте и порядке. Мусор и упаковочный материал должны быть незамедлительно удалены и вывезены на место, которое указано Kcell.
12. Аварийное оборудования или зона эвакуации в случае пожара не должны быть заблокированы в результате деятельности Поставщика.
13. Поставщик должен провести для своего персонала обучение технике безопасности перед началом работ в помещениях Kcell.

5.9 Оперативная безопасность

1. Поставщик должен иметь действующую систему управления изменениями для внесения изменений в бизнес процессы, Средства обработки информации объектов и системы. Система управления изменениями включает в себя тесты и обзоры, предшествующие внедрению изменений, например: процедуры по обработке срочных изменений; процедуры по возврату в исходное состояние после безуспешных изменений; журналы, отражающие внесенные изменения и кем и когда они были внесены.
2. Поставщик должен иметь систему защиты от вредоносных программ, чтобы гарантировать, что любое программное обеспечение, используемое для предоставления Поставщиком услуг/материалов по Соглашению в пользу Kcell, защищено от вредоносных

exceptions, faults and information security events and regularly review these. Furthermore, the Supplier shall protect and store (for at least 6 months) Log information, and on request, deliver monitoring data to the Kcell. 5. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner. 6. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications. 7. The Supplier shall ensure development is segregated from test and production environment.	программ. 3. Поставщик должен создавать резервные копии важной информации, а также проводить тестирование резервных копий с целью восстановления информацию по согласованию с Kcell 4. Поставщик обязан Вести учет и осуществлять мониторинг действий пользователя, исключений, ошибок и событий информационной безопасности и регулярно проверять их. Кроме того, Поставщик должен обеспечивать защиту и хранение (в течение не менее 6 месяцев) Учетной информации и по запросу передавать данные мониторинга в Kcell. 5. Поставщик должен активно и своевременно управлять факторами уязвимости в отношении всех соответствующих технологий, таких как операционные системы, базы данных, приложения. 6. Поставщик должен установить базовые уровни безопасности (усиление защиты) для всех соответствующих технологий, таких как операционные системы, базы данных, приложения. 7. Поставщик должен обеспечить разграничение между тестовой и производственной средой.
5.10 Communications security 1. The Supplier shall implement network Security Controls such as service level, firewalling and segregation to protect information systems. 2. The Supplier shall ensure that voice communication classified as confidential and secret (as further detailed below) is secure this means that un-encrypted communication may not be used.	**5.10 Безопасность связи** 1. Поставщик должен внедрить средства контроля над сетевой безопасностью, такие как уровень обслуживания, межсетевой экран и сегрегация для защиты информационных систем. 2. Поставщик должен обеспечить защиту и безопасность голосовой коммуникации, отнесенной к категории конфиденциальной и секретной информации (как более подробно описано ниже), т.е. запрещено использование связи без шифрования.
5.11 System acquisition, development and maintenance (when software development or system development is provided to the Kcell by Supplier) 1. The Supplier shall implement rules for development lifecycle of software and systems including change and review procedures. 2. The Supplier shall test security functionality during development in a controlled environment.	**5.11 Приобретение, разработка и сопровождение системы (при разработке Поставщиком программного обеспечения или системы для Kcell)** 1. Поставщик должен внедрить правила для всего жизненного цикла разработки программного обеспечения и систем, включая процедуры изменения и обзора. 2. Поставщик обязан протестировать функции безопасности в процессе разработки в контролируемой среде.
5.12 Supplier relationship with sub-suppliers 1. The Supplier shall reflect the content of these Security Directives in its agreements with sub-suppliers that perform tasks assigned under the Agreement. 2. The Supplier shall regularly monitor, review and audit sub-supplier‘s compliance with the Security Directives. 3. The Supplier shall, at the request of the Kcell, provide the Kcell with evidence regarding sub-supplier’s compliance with the Security Directives.	**5.12 Отношения Поставщикам с субподрядчиками** 1. Поставщик должен отражать содержание настоящих Директив по безопасности в договорах с субподрядчиками, привлеченными к выполнению задач в соответствии с Соглашением. 2. Поставщик обязан регулярно контролировать, анализировать и проводить проверку соблюдения субподрядчиками требований Директив по безопасности. 3. Поставщик обязан, по требованию Kcell, предоставить доказательства соблюдения субподрядчиками требований Директив по безопасности.
5.13 Security Incident management	**5.13 Управление инцидентами безопасности**

1. The Supplier shall have established procedures for Security Incident management. 2. The Supplier shall report security related incidents to the Kcell without any unjustified delay in an effective and accurate manner. 3. The Supplier shall provide the Kcell with support in case of forensic investigation.	1. Поставщик должен иметь действующие процедуры по Управления инцидентами безопасности. 2. Поставщик обязан своевременно и точно сообщать Kcell об инцидентах, связанных с нарушением безопасностью, без необоснованной задержки. 3. Поставщик должен оказывать содействие Kcell при проведении судебной экспертизы.
5.14 Business continuity management 1. The Supplier shall identify business continuity risks and take necessary actions to control and mitigate such risks. 2. The Supplier shall have documented processes and routines for handling business continuity. 3. The Supplier shall periodically assess the efficiency of its business continuity management, and compliance with availability requirements (if any). 4. The Supplier shall regularly test measures securing the delivery of services if such are put in place.	**5.14 Управление непрерывностью бизнеса** 1. Поставщик должен выявлять риски, связанные с непрерывностью бизнеса, и принимать необходимые меры для контроля и снижения таких рисков. 2. Поставщик должен иметь документально оформленные процессы и процедуры для обеспечения непрерывности бизнеса. 3. Поставщик должен периодически проводить оценку эффективности управления непрерывностью бизнеса и соблюдение требований по доступности (при наличии таковых). 4. Поставщик должен регулярно проверять меры по обеспечению оказания услуг, при их наличии.
5.15 Compliance 1. The Supplier shall comply with all relevant legislation and contractual requirements including but not limited to Personal Data protection. 2. The Supplier shall, on request, provide the Kcell with a compliance status report with regards to these Security Directives without any unjustified delay. **3.** The Kcell has the right to audit how the Supplier and its sub-suppliers fulfil the Security Directives or corresponding requirements.	**5.15 Соблюдение требований** 1. Поставщик должен соблюдать все соответствующие законодательные акты и договорные требования, включая, но не ограничиваясь этим, защиту Персональных данных. 2. Поставщик должен, по запросу, предоставить Kcell отчет о соблюдении требований, установленных настоящими Директивами по безопасности без необоснованной задержки. **3.** Kcell вправе проверять Поставщика и его субподрядчиков на предмет выполнения Директив по безопасности или иных соответствующих требований.
6 IT SECURITY The Supplier's environment 1. The Supplier's hardware and/or software which are used for processing Kcell's information shall have appropriate information security protection in place, as set forth by legislation, regulations and industry best practise (e.g. Security administration routines for malware protection, Patch management, User authentication, Access control, Confidentiality protection, Incident detection, Log management , Disaster recovery, Key management, Network security management and Physical protection of IT-resources). 2. Services or software harmful for the processing of data or the operation of the system shall not be installed or active in the systems used for performing the tasks defined in the agreement. 3. Systems storing and processing data shall be set up and "hardened" according to the software vendor's recommendation and best practices. 4. The Supplier shall have a continuity plan for the production environment used when providing services. 5. The Supplier shall ensure that the Supplier's own	**6 IT БЕЗОПАСНОСТЬ** **Требования к ресурсам Поставщика** 1. Оборудование и/или программное обеспечение Поставщика, которые используются для обработки информации Kcell, должны иметь соответствующую действующую защиту информации от несанкционированного доступа, как это предусмотрено законодательством, положениями и передовыми отраслевыми практиками (например, программы управления безопасности для защиты от вредоносного ПО, управление программными вставками, аутентификация пользователей, контроль доступа, защита от раскрытия информации, обнаружение и регистрация аварийных ситуаций, управление журналами регистрации, обеспечение функционирования в случае чрезвычайных ситуаций, управление ключами, управления безопасностью сети и физическая защита IT-ресурсов). 2. Сервисы или программное обеспечение, наносящие вред данным при их обработке или являющиеся губительными для работы системы, не должны устанавливаться или активизироваться в системах, используемых для выполнения задач, определённых в договоре.

environments used for functions specified in the agreement are monitored in such a manner that events violating information security are detected and traceable to a specific person. If agreed between Kcell and Supplier, monitoring data shall be transferred to Kcell.

6. The Supplier shall ensure that backups of the information processed on behalf of Kcell by the Supplier are taken, and that such backups are restorable when the information is handled in the Supplier's environment.
7. Backup copies shall be handled with the same confidentiality as the original data. Backup copies shall be stored separated from the original data to prevent simultaneous destruction of both original data and the backup copy in a disaster situation.
8. The Supplier shall keep audit trails according to legislation or as otherwise defined in the agreement. The Kcell must, without delay, get access to relevant audit trails relating to the Kcell when managing security incidents.
9. System administrators or other high privilege users shall authenticate using strong authentication (2-factor).
10. Remote access users shall be authenticated using strong authentication when accessing the system from untrusted networks.
11. Laptops and removable media shall be encrypted if used or moved outside of the Suppliers facilities.

Kcell's environment

1. Equipment and IT functionality supplied by Kcell shall only be used for performing agreed services.
2. Equipment and IT functionality supplied by Kcell shall be handled according to Kcell's instructions.
3. The Supplier shall protect Kcell assets in its care from accidental losses or theft.

3. Системы хранения и обработки данных должны быть разработаны и усилены в соответствии с рекомендациями поставщика программного обеспечения и передовыми практиками.
4. Поставщик должен иметь план обеспечения непрерывности функционирования производственного оборудования, используемого при предоставлении услуг.
5. Поставщик должен предоставить гарантии в том, что собственные ресурсы Поставщика, используемые для осуществления функций, указанных в договоре, контролируются таким образом, что события нарушения информационной безопасности могут быть обнаружены и отнесены к конкретному лицу. По согласованию между Kcell и Поставщиком, данные мониторинга передаются Kcell.
6. Поставщик обязан обеспечить резервное копирование информации, обрабатываемой от имени Kcell Поставщиком, и возможность восстановления таких резервных копий при обработке информации в среде Поставщика.
7. Резервные копии должны обрабатываться с соблюдением аналогичных требований соблюдения конфиденциальности, как и при обработке исходных данных. Резервные копии должны храниться отдельно от исходных данных для предотвращения одновременного уничтожения, как исходных данных, так и резервных копий, при возникновении чрезвычайной ситуации.
8. Поставщик обязан хранить журналы регистрации событий в соответствии с законодательством или иным образом, как определено в договоре. Kcell должно незамедлительно получить доступ к соответствующим журналам регистрации событий, имеющих отношение к Kcell, при рассмотрении и урегулировании инцидентов информационной безопасности.
9. Системные администраторы и другие высокопривилегированные пользователи должны осуществлять аутентификацию с использованием строгой (2-х факторной) аутентификации.
10. Пользователи удалённого доступа устанавливаются с использованием строгой аутентификации при доступе к системе из ненадёжных сетей.
11. Ноутбуки и переносные носители подлежат шифрованию при использовании или перемещению за пределы помещений Поставщика.

6.2 требования к ресурсам Kcell

1. Оборудование и ИТ-функциональность, предоставляемые Kcell, должны использоваться только для выполнения согласованных услуг.
2. Оборудование и IT-функциональность, предоставляемые Kcell, должны эксплуатироваться в соответствии с инструкциями Kcell.
3. Поставщик должен обеспечить защиту активов Kcell, при оказании поддержки в защите от случайной потери или

6.1 INFORMATION SECURITY

1. The Supplier shall ensure the security of information handled by the Supplier and related to Kcell. The Supplier shall act diligently and according to applicable local law when handling Kcell's information.
2. All Confidential Information provided by Kcell must, when handled by the Supplier, be subject to the following rules:
   - Paper documents, removable media etc., shall be kept in safe control of an authorized person and handled according to Kcell's Security Classification instruction or according to Kcell's general information security procedures.
   - Voice communication of information belonging to Kcell shall be performed in a secure manner. This means inter alia that analogue wireless telephone systems, unencrypted public IP telephony or unencrypted communication radio may not be used. Communicating information from public premises is not allowed.
   - Data communication of Kcell information shall be performed in a secure manner (e.g. using end to end encryption during transmission, using communication links trusted by Kcell or using security measures in generally used software). Exception from this rule requires Kcell's written consent.
   - The Supplier's Personnel may under no circumstances deliberately try to access information not needed for the assignment agreed upon, or information for which the Supplier's Personnel is not granted access. If any person of the Supplier's Personnel unintentionally gains unauthorized access to information, this shall promptly be reported to Kcell.
3. Regarding handling of information, the Supplier is only allowed to copy or reproduce information on data files, hard copy or other tangible media as part of tasks performed for the Kcell.
4. The person producing copies for personal use (working copy) is responsible for their destruction when they are not to be used anymore.
5. Copy or reproduction shall not be done in such a way that marking of owner of information or security class is removed.
6. The Supplier shall always handle information on data files, hard copy or other tangible media in such a way that considerable effort is required from unauthorized persons to gain access to the information, regardless of if the information is handled within the Supplier's premises or not.
7. The Supplier shall ensure that the information handled by the Supplier and related to the agreement is not mixed with information not related to the agreement.
8. Data used in production shall never be used in development or test. However, if test data cannot be used, the system shall comply to the same security requirements as the

6.1 Информационная безопасность

1. Поставщик должен обеспечить безопасность информации, обрабатываемой Поставщиком и относящейся к АО «Кселл». Поставщик обязан действовать добросовестно и в соответствии с местными законами при обработке информации АО «Кселл».
2. Вся Конфиденциальная информация, предоставленная АО «Кселл», должна соответствовать следующим требованиям при её обработке Поставщиком:
   - Документы на бумажных носителях, съёмные носители информации и т.д., должны храниться под строжайшим контролем уполномоченного лица и обрабатываться в соответствии с Инструкцией по определению грифа секретности АО «Кселл или в соответствии с общими процедурами информационной безопасности АО «Кселл».
   - Голосовая передача информации, относящейся к АО «Кселл», должна осуществляться с соблюдением режима безопасности. Это означает, среди прочего, что аналог беспроводных телефонных систем, нешифрованная общедоступная IP-телефония или нешифрованная радиосвязь не могут быть использованы. Передача информации от общественных помещений не допускается.
   - Передача данных АО «Кселл» осуществляется в безопасном режиме (например, с использованием сквозного шифрования при передаче, с использованием каналов связи, в которых АО «Кселл» уверен, или с использованием мер безопасности, которые обычно использует программное обеспечение). Исключение из этого правила требует письменного согласия АО «Кселл».
   - Персонал Поставщика не вправе ни при каких обстоятельствах намеренно пытаться получить доступ к информации, в которой нет необходимости для выполнения согласованного задания, или к информации, в отношении которой персоналу Поставщика доступ не предоставляется. В случае если любой сотрудник из числа Персонала Поставщика непреднамеренно получит несанкционированный доступ к информации, то АО «Кселл» должен быть незамедлительно уведомлён об этом.
3. Относительно обработки информации Поставщику разрешено только копирование и воспроизведение информации, хранящейся в файлах данных, на печатных носителях или других материальных носителях в рамках задач, выполняемых для АО «Кселл».
4. Лицо, производящее копии для личного пользования (рабочая копия), несёт ответственность за их уничтожение, если они больше не будут использоваться.
5. Копирование или воспроизведение не должны повлечь за собой удаление маркировки собственника информации

кражи.

production system. 9. Obtaining information for test purposes from a production environment always requires Kcell's written consent. **10.** At the ceasing of the agreement, or when an assignment no longer requires processing of data, the Supplier shall deliver all data which is related to the processing performed on behalf of Kcell to the Kcell or, to the extent not possible, certify destruction of the same.	или категории безопасности. 6. Поставщик должен при всех обстоятельствах обрабатывать информацию, хранящуюся в файлах данных, на печатных носителях или других материальных носителях, таким образом, чтобы посторонним лицам потребовались значительные усилия для получения доступа к информации, независимо от того, обрабатывается ли информация в помещениях Поставщика или нет. 7. Поставщик гарантирует, что информация обрабатывается Поставщиком, и что информация, относящаяся к договору, не смешивается с информацией, не связанной с договором. 8. Данные, используемые в производстве, ни при каких обстоятельствах не должны использоваться для разработки или тестирования. Вместе с тем, если тестовые данные не могут быть использованы, то система должна отвечать аналогичным требованиям безопасности, которые применяются в отношении производства. 9. Получение информации в целях тестирования из области производства допускается только с письменного согласия АО «Кселл». 10. При прекращении договора, или если выполнение задания больше не требует обработки данных, Поставщик обязан передать АО «Кселл» все данные, которые связаны с обработкой, выполняемой от имени АО «Кселл», или, насколько это невозможно, предоставить свидетельство её уничтожения.
7 Information Security Confidentiality class description and handling requirements	**7 Описание классов конфиденциальности и правила обращения с конфиденциальной информацией**

Class/ Класс	Description / Описание	Examples of information types / Примеры типов информации
Secret / Секретная	The unauthorized access or disclosure of information could **seriously damage Kcell**, its organization, critical functions, workforce, business partners and/or its customers / Несанкционированный доступ или раскрытие информации может нанести **серьезный ущерб** Kcell, ее организации, критически важным функциям, рабочей силе, деловым партнерам и / или клиентам.	- annual report and result before they have been released - certain information based on legal requirements or specific customer agreements or non-disclosure agreements / - годовой отчет и результаты деятельности до их официального опубликования - определенная информация правового характера, некоторых договоров с клиентами или соглашения о неразглашении конф. информации
Confidential / Конфиденциальная	The unauthorized access or disclosure of information could **damage** Kcell, its organization, critical functions,	- certain information based on legal requirements e.g. personal data of customers or employees - sensitive business plans, strategies and decisions (e.g.

	workforce, business partners and/or its customers. / Несанкционированный доступ или раскрытие информации может **нанести ущерб** Kcell, ее организации, критически важным функциям, рабочей силе, деловым партнерам и / или клиентам.	marketing plans) / - определенная информация правового характера, например, личные данные клиентов или сотрудников - конфиденциальные бизнес-планы, стратегии и решения (например, маркетинговые планы)
Internal / Внутренняя	The unauthorized access or disclosure of information could cause **minor damage** Kcell, its organization, critical functions, workforce, business partners and/or its customers. / Несанкционированный доступ или раскрытие информации может нанести **незначительный ущерб** Kcell, ее организации, критически важным функциям, рабочей силе, деловым партнерам и / или клиентам.	- information that is meant for Kcell's internal use - communication materials targeted to all Kcell employees e.g. related to Kcell organization, strategy, products, employee services / - информация, предназначенная для внутреннего использования Kcell - информационные материалы, предназначенные для сотрудников Kcell например, связанные с организацией, стратегией, продукцией, обслуживанием сотрудников
Public / Публичная	The unauthorized access or disclosure of information causes **no damage** Kcell, its organization, critical functions, workforce, business partners and/or its customers. / Несанкционированный доступ или раскрытие информации **не наносит никакого ущерба** Kcell, ее организации, критически важным функциям, рабочей силе, деловым партнерам и / или клиентам.	- annual report and result after they have been released - marketing materials and press releases that are published - information that needs to be published based on legal requirements / - годовой отчет и результаты деятельности после их официального опубликования - опубликованные маркетинговые материалы и пресс-релизы - информация, разглашаемая в соответствии с законодательными требованиями

Class	**Who may access the information**	**How to store**	**How to transfer**	**How *to* use**	**How to assess need for protection (risk based approach)**
Класс	**Кто может получить доступ к информации**	**Как хранить**	**Как передавать**	**Как использовать**	**Как оценить необходимость в защите (подход, основанный на рисках)**

Secret	Appointed persons only	Logically and physically secure storage i.e. encrypted or locked	Through secure communication channels or in a secure portable storage (locked)	To be used within secure areas that are protected from insight and eavesdropping (by unauthorized persons)	It shall be very hard to break the protection. Only highly motivated and/or resourceful attackers could dismantle the protection.
Секретная	Только назначенные лица	Логически и физически безопасное хранение, т.е. шифрование или блокировка доступа	По защищенным каналам связи или на защищенном портативном накопителе (в заблокирован виде)	Для использования в безопасных областях, защищенных от проникновения и прослушивания (посторонними лицами)	Защита должны быть устойчивой к взлому. Только сильно заинтересованные и/или изобретательные злоумышленники способны взломать защиту.
Confidential	A limited *and controlled* group of persons only	Logically and physically controlled and trusted storage* with strict access control	Through secure communication channels or within a controlled and trusted network, or in a secure portable storage*	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping (by unauthorized persons)	It shall be hard for unauthorized persons to get access to the information. Only well motivated attackers could dismantle the protection.
Конфиденциальная	Только ограниченная и *контролируемая* группа лиц	Логически и физически контролируемое хранение* при строгом контроле доступа	По защищенным каналам связи или по контролируемой и надежной сети, или на защищенном портативном накопителе*	Для использования уполномоченными лицами в коммерческих целях только в пределах контролируемого рабочего пространства или места, защищенного от проникновения и прослушивания (посторонними лицами)	Посторонним лицам трудно получить доступ к информации. Только заинтересованные злоумышленники способны взломать защиту.

Internal	Those who perform work for Kcell JSC	Under logical and physical access control	Through protected communication channels or within a trusted network	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping (by unauthorized persons)	It shall be unlikely for unauthorized persons to get access to the information. Only motivated attackers could dismantle the protection.
Внутренняя	Те, кто выполняет работу для АО “Кселл”	Логический и физический контроль доступа	По защищенным каналам связи или по контролируемой и надежной сети	Для использования уполномоченными лицами в коммерческих целях только в пределах контролируемого рабочего пространства или места, защищенного от проникновения и прослушивания (посторонними лицами)	Возможность для посторонних лиц получить доступ к информации маловероятна. Только заинтересованные злоумышленники способны взломать защиту.
Public	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions
Публичная	Без ограничений	Без ограничений	Без ограничений	Без ограничений	Без ограничений