＜業者登録時＞

成田国際空港株式会社（以下、「甲」という。）が発注を予定する入札、見積書提出、受注等（以下、「受注等」という。）にあたり、貴社名を入力してください（以下、「乙」という。）が取扱う甲の秘密情報の安全管理に関し、必要な事項を以下の通り定め、遵守することを誓約する。

様式２-２

千葉県成田市成田国際空港内ＮＡＡビル

成田国際空港株式会社

代表取締役社長　藤井　直樹　殿

秘密情報の安全管理に関する誓約書

（秘密情報）

第１条　本誓約書において、秘密情報とは、文書、電磁的方法、口頭その他媒体を問わず、次の各号のいずれかに該当するものとする。

1. 本件の過程において知り得た、甲の技術上の情報、営業上の情報、その他一切の業務上の情報
2. 受注等に係る個人情報
3. 受注等の過程において乙が知り得た制限区域内の図面等航空保安上重要な情報

２　前項に規定する情報のうち、甲から書面による承諾を事前に得た場合又は次の各号のいずれかに該当する場合は秘密情報とはしないものとする。ただし、前項第２号に規定する個人情報を除くものとする。

* 1. 知得した時点で既に公知となっていた情報
  2. 知得した時点で既に保有していた情報（ただし、秘密情報として取扱われている情報を除く。）
  3. 知得した後に乙の責めに帰すべからざる事由により公知となった情報
  4. 正当な権利を有する第三者から秘密保持義務を負うことなく適法に入手した情報
  5. 甲からの情報によらず独自に開発したもの

（秘密保持義務）

第２条　乙は、秘密情報を秘密として保持し、次の各号のいずれかに該当する場合を除き、甲の書面による事前の同意なくして、これを第三者に提供又は開示してはならないものとする。また、秘密情報を、受注等を遂行する目的以外に使用してはならないものとする。

1. 法令等に基づき、裁判所、政府機関その他の公的機関から秘密情報を開示することを要求された場合。ただし、実務上可能な範囲で事前又は事後に相手方に通知するものとし、かつ開示範囲を合理的に必要な限度に留めるよう努力するものとする。
2. 受注等に基づく業務行為に必要な限りにおいて、自社の役員及び従業員（派遣労働者等を含む。）に対し、本誓約書と同等の義務を課した上で開示する場合
3. 必要があるときに、弁護士、税理士等法令上守秘義務を負う者に対して開示する場合

２　乙は、受注等に関わり秘密情報を取扱う必要のある自社の役員及び従業員（派遣労働者等を含む。）に対して、在職中及び退職後も前項の規定を遵守させ、それに関する教育指導その他必要な措置を講じるものとする。

３　乙が甲の書面による事前の同意を得て第三者に秘密情報を開示する場合は、乙は当該第三者との間で本誓約書と同等の秘密保持契約を締結して秘密保持義務を遵守させるものとし、当該第三者による秘密情報の取扱いについて一切の責めを負う。

（秘密情報の取扱い）

第３条　乙は、秘密情報を取扱う際には、次の各号に掲げる事項を遵守する。

1. 受注等の遂行に必要な範囲を超えて秘密情報を取得、利用又は加工しないこと
2. 秘密情報の複製及びその範囲は、甲の事前の許諾によること
3. 秘密情報を厳重に管理し、漏洩、改ざん、滅失、き損又はその他の事故を防止すること
4. 受注等の目的に関わる使用が終了し、又は本誓約書が解除された場合、もしくは甲から秘密情報の返還請求を受けたときは、速やかに、秘密情報及びこれに関連する一切の資料を甲へ返還し、返還が困難な場合には、当該資料を消去又は廃棄すること
5. 前各号に掲げる事項のほか、秘密情報の管理及び利用のために必要な措置をとること

（安全管理措置）

第４条　乙は、秘密情報及びその複製物を善良な管理者の注意義務をもって保管するものとし、その取扱いにつき、次の各号に掲げる安全管理措置を講じるものとする。

1. 秘密情報管理責任者の設置等組織体制の整備
2. 秘密情報の保管場所の施錠、入退室管理、建物及び機器等の災害対策並びに外部持ち出しの制限等の物理的セキュリティ
3. 電磁的方法により記録された秘密情報に対してのアクセスコントロール及びバックアップ等の技術的セキュリティ
4. 個人所有のパソコン、ファイル交換ソフトがインストールされているパソコン又は有効なウイルス対策ソフトがインストールされていないパソコンの使用禁止
5. 関係者に対する教育・訓練
6. 秘密情報の機密性、完全性、又は可用性が侵害される事態（以下、「事故」という。）が発生し又は発生するおそれがある場合の甲に対する連絡、報告等についての体制の整備

（報告及び調査）

第５条　甲が次の各号に掲げる措置をとろうとする場合、乙はこれに協力する。

1. 定期又は随時に秘密情報の取扱状況につき報告を求めること
2. 事前に乙が了解をし、乙の立会いのもとで、受注等の履行に関連する乙の事業所内作業場所に立ち入り、秘密情報の管理状況を確認すること
3. 前２号の調査の結果、甲が不都合と認めた事項について、乙に改善を求めること

（事故対応）

第６条　乙は、秘密情報について、漏洩、窃盗、滅失、き損などの事故が発生し又は発生するおそれがある場合、甲に対してその事実関係について速やかに報告し、甲の指示に従うものとする。受注等が終了した後においても、同様とする。

（損害賠償）

第７条　乙が、本誓約書に定める事項に違反したことにより、甲或いは第三者に損害を与えた場合、当該損害を賠償するものとする。

（個人情報）

第８条　乙は、秘密情報が個人情報に該当する場合には、前各条に定めるもののほか、個人情報の保護に関する法律等（関連する諸法令及び個人情報の保護に関するガイドラインを含む。）を遵守し、個人の権利利益を侵害しないものとする。

（再委託等）

第９条　乙は、受注等の一部を第三者に委託させ又は請け負わせようとする場合には、甲の書面による事前の同意を得るものとし、当該第三者に対して、秘密情報の取扱いにつき、本誓約書と同様の安全管理措置義務を負わせ、監督し、かかる秘密保持義務違反について、責任を負うものとする。

（協議）

第10条　本誓約書に定め無き事項その他本誓約書に関する解釈上の疑義は、信義誠実の原則に従い、甲、乙協議の上解決するものとする。

（本誓約書の真正性）

第11条　本誓約書が甲のシステムを経由して乙から甲に提出された場合には、押印を省略した場合であっても、真正に作成された書類として乙から提出されたものとみなす。

申請日を入力してください（西暦年月日）

|  |  |
| --- | --- |
| ［住　　所］ | 住所を入力してください |
| ［社　　名］ | 貴社名を入力してください |
| ［代表者名］ | 役職 代表者氏名を入力してください |

情報セキュリティ管理体制（１/３）

|  |
| --- |
| 1. 情報セキュリティ対策等の具体的な取組内容 |
| （記載方法）・情報管理及び情報事故に関する具体的な取組内容を記載すること。  ※情報セキュリティに係る社内規程・細則等が定まっている場合は、その全ての名称及び制定日などを記載するだけで良い。 |
| 1. 紛失・盗難対策  |  | | --- | | （例）紛失・盗難に備えて、パソコンのパスワード設定およびハードディスクやデータの暗号化を実施している。 |  1. Web誤公開・メール等の誤送信対策  |  | | --- | | （例）WEBサイトへの誤公開、メール誤送信に対する対策が講じられている。 |  1. 内部不正対策  |  | | --- | | （例）適切なアクセス権限設定が行われている。入退室管理が身分証明書等によりその都度確認されている。社員への情報セキュリティ教育が実施されている。 |  1. シャドーIT対策  |  | | --- | | （例）クラウドサービスについては許可制であり、会社が許可したクラウドサービス以外の使用はできないような設定を行っている。 |  1. 不正プログラム・脆弱性対策  |  | | --- | | （例）マルウェア対策ソフトをインストールし、パターンファイルの更新が適切に行われている。OSや使用するソフトウェアの更新プログラムを適用しており、脆弱性対策を行っている。 |  1. 不正アクセス対策  |  | | --- | | （例）情報への不正なアクセスを防止する機能を設け、且つ検出できる仕組み（ログ保存等）を講じている。 | |

情報セキュリティ管理体制（２/３）

|  |
| --- |
| ②情報漏洩事故等が発生した時の対応フロー |
| （記載方法）・情報漏洩事故等が発生した時の対応フロー図を記載すること。  ※情報セキュリティに係る社内規程・細則等が定まっている場合は、その全ての名称及び制定日などを記載するだけで良い。 |
| 【ステップ１】事故の発見及び報告   |  | | --- | | （例）事故の発見後、直ちに関係者への一次報告を行う。 |   【ステップ２】初動対応（事実確認の実施）   |  | | --- | | （例）何の情報が、何件、何時、どこから、どの様に、何故漏洩したか事実確認を行うと共に応急措置を実施する。 |     【ステップ３】詳細調査   |  | | --- | | （例）漏洩した情報区分（個人情報／取引相手先の社内情報など）、影響範囲（個人／取引相手先の会社）、情報の保護策を実施していたか、情報管理上の問題点は何かを調査し、想定されるリスク並びに被害の重要度を判定する。 |     【ステップ４】関係者への通知   |  | | --- | | （例）二次被害防止のため漏洩した情報区分、情報量、影響範囲等について関係者へ通知を行うと共に関係者の意向に合わせた対応を行う。 |     【ステップ５】事後対応   |  | | --- | | （例）再発防止策の検討を行い関係者（個人／取引相手先など）への説明を行う。 | |

情報セキュリティ管理体制（３/３）

|  |
| --- |
| ③情報漏洩事故等が発生した時の連絡体制表 |
| （記載方法）・情報漏洩事故等が発生した時の連絡体制表を記載すること。 |
| |  | | --- | | 情報漏洩  事故等が発生  ・紛失・盗難  ・誤公開、誤送信  ・情報漏洩が伴うサイバー攻撃など |  |  | | --- | | 貴社名を入力してください  【 担当者 】  CYDEENの個別情報登録における申請者のとおり  【 情報セキュリティ事故　対策チーム 】  情報管理に関する担当部署名を記載してください（例：総務部総務課）  　TEL 上記担当部署の電話番号を記載してください（例：0476-34-0000） |  |  | | --- | | 契約前：ＮＡＡ契約担当者 TEL 0476-34-5484/5145  ~~契約後：監督員又は調査職員 TEL~~ | |