7.2　雇用期間中

目的：従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため

7.2.1　経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。

7.2.1.1　経営陣の責任には、従業員及び契約相手に、秘密情報又は情報システムへのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備することを含める。

7.2.1.2　経営陣の責任には、従業員及び契約相手に、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備することを含める。

7.2.1.3　経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備することを含める。

7.2.1.4　経営陣の責任には、従業員及び契約相手に、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備することを含める。

7.2.1.5　経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備することを含める。

7.2.1.6　経営陣の責任には、従業員及び契約相手に、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備することを含める。

7.2.1.7　経営陣の責任には、従業員及び契約相手に、情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備することを含める。

7.2.1.8　経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動する。

7.2.2　組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。

7.2.2.1　情報セキュリティの意識向上プログラムは、従業員、及び関係する場合は契約相手に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させることを狙いとする。

7.2.2.2　情報セキュリティの意識向上プログラムは、保護すべき組織の情報及び情報を保護するために実施されている管理策を考慮に入れて、組織の情報セキュリティのための方針群及び関連する手順に沿って確立する。

7.2.2.3　情報セキュリティの意識向上プログラムには、キャンペーン（例えば、情報セキュリティの日）、及びパンフレット又は会報の発行のような、複数の意識向上活動を含める。

7.2.2.4　情報セキュリティの意識向上プログラムは、組織における従業員の役割、及び関係する場合には契約相手の認識に対する組織の期待を考慮に入れて、計画する。

7.2.2.5　情報セキュリティの意識向上プログラムの活動は、新しい従業員及び契約相手も対象とされるよう、長期にわたり、できれば定期的に計画する。

7.2.2.6　情報セキュリティの意識向上プログラムは、定期的に更新して組織の方針及び手順に沿って、情報セキュリティインシデントから学んだ教訓が生かされるようにする。

7.2.2.7　意識向上のための訓練は、（例えば、教室での訓練、通信教育、インターネットを利用した訓練、自己学習その他を含む、多様な手段を用いて、）組織の情報セキュリティの意識向上プログラムで必要とされた場合に実施する。

7.2.2.8　情報セキュリティの教育及び訓練には、組織全体にわたる情報セキュリティに対する経営陣のコミットメントの提示を含める。

7.2.2.9　情報セキュリティの教育及び訓練には、方針、規格、法令、規制、契約及び合意で定められた、適用される情報セキュリティの規則及び義務を熟知し、これを順守する必要性を含める。

7.2.2.10　情報セキュリティの教育及び訓練には、自身が行動したこと及び行動しなかったことに対する個人の責任、並びに組織及び外部関係者に属する情報のセキュリティを保つか、これを保護することに対する一般的な責任を含める。

7.2.2.11　情報セキュリティの教育及び訓練には、情報セキュリティに関する基本的な手順（例えば、情報セキュリティインシデントの報告）及び基本的な管理策（例えば、パスワードのセキュリティ、マルウェアの制御、クリアデスク）を含める。

7.2.2.12　情報セキュリティの教育及び訓練には、情報セキュリティに関連する事項についての追加的な情報及び助言（情報セキュリティの教育及び訓練に関する追加の資料も含む。）を得るための連絡先及び情報源を含める。

7.2.2.13　情報セキュリティの教育及び訓練は、定期的に実施する。

7.2.2.14　最初の教育及び訓練は、新入社員だけでなく、情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用し、その役割が始まる前に実施する。

7.2.2.15　組織は、教育及び訓練を効果的に実施するためのプログラムを開発する。

7.2.2.16　教育及び訓練を効果的に実施するためのプログラムは、保護する必要のある組織の情報及び情報を保護するために実施されている管理策を考慮に入れるプロセスを含める。

7.2.2.17　教育及び訓練を効果的に実施するためのプログラムは、組織の情報セキュリティのための方針群及び関連手順に沿っている。

7.2.2.18　教育及び訓練を効果的に実施するためのプログラムでは、講義又は自己学習のように、多様な教育及び訓練の形式を考慮して、定める。

7.2.3　情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。

7.2.3.1　懲戒手続は、情報セキュリティ違反が生じたことの事前の確認を待って開始する。

7.2.3.2　正式な懲戒手続には、情報セキュリティ違反を犯したという疑いがかけられた従業員に対する正確かつ公平な取扱いを含める。

7.2.3.3　正式な懲戒手続は、違反の内容及び重大さ並びにその業務上の影響、最初の違反か又は繰り返されたものか、違反者は、適切に教育・訓練されていたかどうか、関連する法令、取引契約、その他の必要な要素を考慮した段階別の対応を定める。

7.2.3.4　懲戒手続を、従業員が情報セキュリティ違反（従業員による組織の情報セキュリティのための方針群及び手順への違反並びに他の全ての情報セキュリティ違反）を起こすことを防ぐための抑止力として使う。

7.3　雇用の終了及び変更

目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため

7.3.1　雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。

7.3.1.1　雇用の終了に関する責任の伝達には、実施中の情報セキュリティ要求事項及び法的責任、並びに適切であれば、従業員又は契約相手の、雇用の終了以降の一定期間継続する、秘密保持契約及び雇用条件に規定された責任を含める。

7.3.1.2　雇用の終了後も引き続き有効な責任及び義務は、従業員又は契約相手の雇用条件に含める。

7.3.1.3　責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組み合わせとして管理する。