Information Security Policy Statement

Linguitronics Co., Ltd. (hereinafter referred to as the “Company”), adhering to the concept of maintaining information security, provides comprehensive protection and preventive measures for information systems and all data stored, processed, transmitted, or disclosed, so as to eliminate incidents such as damage, theft, leakage, alteration, misuse, and infringement, and to ensure their confidentiality, integrity, and availability (CIA). Accordingly, the Company hereby establishes this Information Security Policy (hereinafter referred to as the “Policy”) as follows, in order to ensure information security, enhance service quality, and achieve the goal of sustainable operation.

Linguitronics

Linguitronics

(1) This Policy shall strictly comply with the personal data protection laws and regulations, copyright laws, and other information security-related laws and regulations applicable in the location of the Company's principal place of business.

(2) Information containing personal data shall be handled with due care in accordance with applicable personal data protection laws, regulations, and related requirements, and may not be privately collected or disclosed to any third party. Access and use are strictly prohibited except as required by law or for official business purposes.

(3) Security regulations shall be established for various information security-related areas, including accounts, information classification, access permissions, data backup, physical security, and environmental security, in order to ensure the confidentiality, integrity, and availability of the Company's information.

(4) Comprehensive response measures shall be established for information security incidents to ensure the continuous operation of information systems and critical business activities.

(5) The Company's information security incident reporting mechanism shall be followed in order to notify relevant stakeholders.

(6) Information security education, training, and awareness promotion shall be conducted to enhance the information security awareness of all personnel and to ensure familiarity with and compliance with relevant information security procedures and regulations.

(7) Personnel are strictly prohibited from privately installing or using software that has not passed review.

(8) Suppliers and contractors shall comply with this Policy and the requirements of the relevant procedures, and may not use or misuse any category of the Company's information assets without authorization. Where sensitive-level or higher business matters are involved, a confidentiality undertaking shall be signed.

(9) A management review meeting shall be convened at least once annually to review the implementation status of the Company's information security operations, establish management indicator measurement standards, and examine the measurement results.

(10) Information asset risk assessments shall be conducted at least once annually, and the acceptable risk level shall be determined by the information security manager.

(11) Drills, testing, and reviews of the business continuity plan and information security incident reporting procedures shall be conducted at least once every six months.

(12) The Company's supervisors shall actively participate in information security management activities and provide support and commitment to information security.

The promulgation of this Policy expressly declares the importance of maintaining information security. All personnel of the Company, as well as suppliers and contractors having business dealings with the Company, shall fully understand this Policy in order to maintain the information security and sustainable operation of all of the Company's business activities.

Information Security Policy Statement

Linguitronics Co., Ltd. (hereinafter referred to as the "Company"), adhering to the concept of maintaining information security, provides comprehensive protection and preventive measures for information systems and all data stored, processed, transmitted, or disclosed, so as to eliminate incidents such as damage, theft, leakage, alteration, misuse, and infringement, and to ensure their confidentiality, integrity, and availability (CIA). Accordingly, the Company hereby establishes this Information Security Policy (hereinafter referred to as the "Policy") as follows, in order to ensure information security, enhance service quality, and achieve the goal of sustainable operation.

Linguitronics

Linguitronics

(1) This Policy shall strictly comply with the personal data protection laws and regulations, copyright laws, and other information security-related laws and regulations applicable in the location of the Company's principal place of business.

(2) Information containing personal data shall be handled with due care in accordance with applicable personal data protection laws, regulations, and related requirements, and may not be privately collected or disclosed to any third party. Access and use are strictly prohibited except as required by law or for official business purposes.

(3) Security regulations shall be established for various information security-related areas, including accounts, information classification, access permissions, data backup, physical security, and environmental security, in order to ensure the confidentiality, integrity, and availability of the Company's information.

(4) Comprehensive response measures shall be established for information security incidents to ensure the continuous operation of information systems and critical business activities.

(5) The Company's information security incident reporting mechanism shall be followed in order to notify relevant stakeholders.

(6) Information security education, training, and awareness promotion shall be conducted to enhance the information security awareness of all personnel and to ensure familiarity with and compliance with relevant information security procedures and regulations.

(7) Personnel are strictly prohibited from privately installing or using software that has not passed review.

(8) Suppliers and contractors shall comply with this Policy and the requirements of the relevant procedures, and may not use or misuse any category of the Company's information assets without authorization. Where sensitive-level or higher business matters are involved, a confidentiality undertaking shall be signed.

(9) A management review meeting shall be convened at least once annually to review the implementation status of the Company's information security operations, establish management indicator measurement standards, and examine the measurement results.

(10) Information asset risk assessments shall be conducted at least once annually, and the acceptable risk level shall be determined by the information security manager.

(11) Drills, testing, and reviews of the business continuity plan and information security incident reporting procedures shall be conducted at least once every six months.

(12) The Company's supervisors shall actively participate in information security management activities and provide support and commitment to information security.

The promulgation of this Policy expressly declares the importance of maintaining information security. All personnel of the Company, as well as suppliers and contractors having business dealings with the Company, shall fully understand this Policy in order to maintain the information security and sustainable operation of all of the Company's business activities.