|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. General  1.1 Purpose  1.2 Scope  1.3 Establishment, revision/repeal, and issuance  1.4 Definitions  2. Ensuring product security    3. Product security operations  3.1 Stipulation of operational rules and promotion of operations  3.2 Determination of products needing security measures  3.3 Risk management  3.4 Product security operations at development, maintenance, and other processes  3.5 Information security measures for the development environment  3.6 Configuration control  3.7 Vulnerability control of procured components that constitute products  3.8 Threat analysis and risk assessment  3.9 Determination of security requirements  3.10 Product security design and implementation    3.11 Confirmation of implementation of product security design  3.12 Planning and implementation of vulnerability verification  3.13 Development of guidelines  3.14 Product security quality maintenance activities  3.15 Handing over to post-development processes  3.16 Management of outsourced external organizations  3.17 Continuous improvement  4. Action against product security incidents  5. Inspection and improvement of operations  6. Control of documents/records  Supplementary provisions | The purpose of these Standards is to supply safe and reliable products by ensuring the security of products in accordance with the “Product Security Operation Rules” (APQ-AY-001) of the Living Appliances and Solutions Company of Panasonic Corporation (hereinafter referred to as “LAS”).  These Standards apply to products and systems that are designed, produced, distributed, or serviced by LAS and divisions (including overseas companies) to whom LAS's quality standards are applied (including services, support tools, libraries, etc. by way of computer applications, smartphone applications, or web applications; with or without fees). The Standards also apply to development for post-shipment changes [version upgrades].  These Standards shall be established, revised, and repealed by the Director of the LAS Quality Innovation Center, and issued by the General Manager in charge of software quality.  For the purpose of these Standards, the following terms shall have the meanings defined in the respective items, except definitions of other terms used in these Standards shall be in accordance with the Operational Rules for Product Security.  (1) Operations related to product security: All operations related to ensuring product security throughout the entire life cycle of products, including planning, design, development, maintenance, etc. that are required for supplying safe and reliable products using information technology (IT)  (2) Products using IT (hereinafter referred to as the “IT Products”): Equipment using networks and other IT, and all service businesses accompanying the equipment.  (3) Vulnerability: Problems in the specifications of IT Products that can be exploited by a third party for an act posing a threat (taking control of a system, leakage of confidential information, etc.)  (4) Known vulnerability: Vulnerability whose existence has been recognized and whose information has been provided  (5) Vulnerability research: To check whether or not vulnerability exists in software and other component parts by gathering public information and information from supplier(s) of component parts  (6) Product security incidents: Both vulnerability that can result in the execution of a malicious attack notified to the company (both disclosed and undisclosed) and actual occurrence of a malicious attack  (7) Risks: Impact of uncertainty on a purpose. For the purpose of these Standards, "risks" means those associated with product security.  (8) Residual risks: Risks that remain after some actions have been taken against original risks and can still affect customers or our business  (9) Security requirements: Requirements that define functions products should have in relation to customer requirements, given characteristics of risks associated with products  (10) Procured components: Components manufactured or possessed by other companies ("Components" include both hardware and software.) that have been acquired by way of purchasing or other legal means (Components whose production is outsourced shall be managed as part of the outsourcing process and excluded from procured components defined hereof.)  (11) Connection: Connection between the product and external devices    In order to ensure the security of IT Products, all processes throughout the entire life cycle of the IT Products must be clarified, and the correlation between the processes and operations related to product security must be identified and managed.  Specific operations and procedures must be implemented with reference to the “Operational Rules for Product Security” and “Operational Standards for Product Security,” as well as relevant guidelines, including the “Product Security - Threat Analysis Guidelines,” “Product Security - Design Guidelines,” Panasonic “Software Development Process Guidelines,” and LAS “Product Security Incident Response Guidelines” (APQ-MQ-003).  Described below are main operations to be conducted to ensure product security.  Divisions shall stipulate product security in-house operational rules in accordance with LAS's rules and standards and promote the operations accordingly.  The Design/Development Department shall take the lead in determining whether an IT Product needs security measures at the software requirement analysis\* (as named in Panasonic “Software Development Process Guidelines”) stage and describe the results in a Planning Policy Sheet (Attachment 1, “Product Planning Operation Standards” [APQ-BD-001]). Security measures shall be taken for IT Products that fall under any of the following criteria. IT Products for which security measures are required by laws/regulations and industrial rules and standards shall also be treated as products needing security measures.  [Criteria]   |  | | --- | | ① Equipped with encryption, authentication, or PKI (Public Key Infrastructure) functions | | ② Equipped with functions for storing/using users’ personal information | | ③ Equipped with functions that use biometrics information | | ④ Equipped with functions for managing/protecting users’ assets (pre-paid information, electronic money, credit information, keys, etc.) | | ⑤ Equipped with functions for protecting copyrights | | ⑥ Equipped with an interface for connecting with IT Products\*  (HDMI, USB, wired/wireless LAN, Wi-Fi, BT, NFC, SD, etc. IT Products that use wired/wireless LAN as an interface are deemed to have network connection functions such as the Internet and Intranet.) | | ⑦ Equipped with functions that allow users to change programs or functions that allow them to do so by using downloaded programs |   \* If an externally undisclosed protocol unique to an IT Product is used for communication among parts of a single IT Product, product security measures are not necessary for such products, as protection is provided within the IT Product.  Divisions shall continuously gather information on products that they are responsible for and, when deemed necessary, manage relevant risks by analyzing and evaluating them. Types of information on risks that need to be continuously gathered include information on laws/regulations and industrial rules and standards, and information contingent to changes in the usage environment, as well as information on new threats and vulnerability.  Should it be difficult to take actions against risks immediately or any risk remain after due actions have been taken, relevant divisions shall manage such risks as residual risks after consultation with the person responsible for implementation of product security operations.  Divisions shall prepare operational standards for product security for their development, maintenance, and other processes. Deliverables from each process shall be prepared and checked in accordance with relevant standards.  Divisions shall maintain information security for the development environment in accordance with rules stipulated by their information system department.  Divisions shall, as part of their configuration control of deliverables from each process, control deliverables related to product security, in order to maintain consistency and integrity of the deliverables of products needing security measures and implement correct design details into products (Example control case: Properly controlling deliverables by keeping versions and baselines of deliverables updated).  Divisions shall control known vulnerability of procured components over the entire product life cycle in order to prevent problems from occurring due to vulnerability of procured components that constitute products. Procured components that are used shall be registered with a system for vulnerability control by AQ2, so as to continuously manage information on vulnerability that may be reported after shipment and take appropriate actions when necessary (Example control case: Conducting research into known vulnerability at the time of accepting procured components, taking actions based on findings from vulnerability information gathered after shipment, etc.)  Divisions shall analyze threats expected of products needing security measures and discuss protection measures that may be necessary for risk assessment, in order to determine product security requirements and manage residual risks.  When analyzing threats and assessing risks, standard techniques/procedures shall be taken. The Product Security Operation Manager shall request relevant departments to conduct threat analysis. In principle, threat analysis shall be conducted by AQ0 and necessary measures shall be completed as well. Threat analysis shall also be conducted when a design change occurs.  If there are no changes in the function to ensure product security from the previous model and the nature of the threat remains unchanged, the analysis results of the previous model may be used for threat analysis of the current model, so long as its reasons are provided. However, when the analysis results of the previous model have been used for three years or longer, a review shall be conducted by taking into account changes in the environment and attack techniques. Such changes in the environment include changes in laws/regulations, industrial rules and standards, and the usage environment, as well as information on new threats and vulnerability.  Divisions shall determine security requirements based on the findings of threat analysis, etc. as stipulated in 3.8 hereof and by taking into account risks associated with product functions and external factors.  Divisions shall conduct design based on the best practices of security design, such as the "Product Security Design Guidelines (TM156)," in order to implement all of the product security requirements determined in 3.9 hereof as intended.  When implementing software, rules that consider security shall be established in the form of coding rules, etc., in accordance with which coding shall be conducted.  Divisions shall conduct static analysis, reviews, and implementation confirmatory tests in order to ensure that product security requirements have been properly implemented into the products they have developed.  The Design/Development Department shall, during the product lifecycle, plan vulnerability verification and ask the Product Security Center or other verification organs to conduct specialized verification for IT Products. Based on the vulnerability verification results, vulnerabilities with a high risk (NG3) shall be eliminated by AQ1. If, for some reasons, such risks cannot be eliminated and remain, separate actions shall be discussed.  <Criteria for vulnerability verification (Results of specialized verification by the Product Security Center)>   |  |  | | --- | --- | | NG3 (high risk) | - Can directly result in information leakage, falsification, failure/restart, taking of control, infection with malware, and falsification (confidentiality/integrity/availability) | | NG2 (medium risk) | - Not directly result in information leakage  - For attacks to be made, limited conditions are necessary (access to a trap page, etc.) | | NG1 (low risk) | - Not directly result in information leakage  - For attacks to be made, more strict conditions than those in NG2 above are necessary | | PD (information provision) | - Does not cause a risk on its own  - Can provide a hint for locating other vulnerabilities |   Divisions shall develop guidelines in order to ensure that users use products needing product security properly and safely. For the purpose of these Standards, guidelines refer to all measures with which to call for attention to users, including, but not limited to, audio, visual, and video instructions, as well as operating instructions, install guides, and other documents.  The following five activities shall be conducted to maintain product security quality of new products throughout the development process, thereby ensuring product security quality at the time of shipment and throughout the product lifecycle.  “Quality maintenance activities” here refers to the “quality maintenance activities” in Attachment 2.   1. Check of the selection of IT Products needing security measures based on the criteria (by Planning Policy, in principle)   - Confirm that the products are selected appropriately in accordance with the criteria   1. Check of the threat analysis results (by AQ0, in principle)   - Confirm that threat analysis has been completed, information assets have been determined, risks have been assessed based on assets and threats, and the need for taking action against threats (document check)   1. Check of evidence that design actions have been taken against threats   - Confirm the check results of the contents of design changes and actions taken subsequently and their impact   1. Check of vulnerability verification results (by AQ1)   - Confirm that actions have been taken against issues thus identified  (Actions against NG3, in particular)   1. Monitoring of product security events throughout the product lifecycle   - Security information on products after shipment shall be gathered by each relevant department. Should vulnerability be reported, necessary actions and improvement efforts shall be made in accordance with the LAS "Product Security Incident Response Guideline" (APQ-MQ-003), thus maintaining product security quality.  Below are key roles and perspectives of the departments involved in each task, including the quality maintenance activities ①～⑤ above. (The following "No." indicates corresponding quality maintenance activities above.)   |  |  |  | | --- | --- | --- | | Tasks | No. | Departments | | Selection of IT Products needing security measures | ① | Element development, design / development | | Threat analysis, product security design, secure coding, static analysis / review and implementation confirmatory tests, vulnerability verification, registration of software in use with the vulnerability management system |  | Element development, design / development | | Confirmation that activities to enhance product security quality are conducted in the development process and that recurrence prevention is taken  Confirmation of security design and the vulnerability verification results |  | Quality, SQA | | Confirmation of evidence of product security quality based on shipment decision documents submitted for mass production prototype study  - That threat analysis has been completed and policies for residual risks have been announced and approved  - That vulnerability verification has been completed  - That high-risk vulnerability (NG3) is absent or has already been dealt with | ②  ③  ④ | *Shinsa* (evaluation) | | Confirmation of threat analysis results, security design, and vulnerability verification results | ②③④ | Department in charge of software quality, Quality Innovation Center | | Monitoring of vulnerability information after shipment and taking of action when an incident occurs | ⑤ | Design / development, quality, SQA, Department in charge of software quality, Quality Innovation Center | | Monitoring and correction of product security measures |  | Quality, SQA |   Divisions shall, in accordance with rules of the information system department, production department, and other relevant departments, appropriately take security measures at the points of production, storage, and distribution after the product has been developed.  Divisions shall, when they outsource their development, maintenance, or other operations regarding products needing product security measures, manage relevant outsourced external organizations, in order to perform product security operations in compliance with their divisional rules (Example control items: selection of outsourced external organizations, requirements at the time of signing a contract, tools used, and what to accept from outsourced external organizations).  When vulnerability verification has found an issue that needs to be improved, etc., measures to mitigate potential threats shall be reflected in design so that such risks may be reduced continuously in future products.  Relevant departments shall, upon receipt of information on product security incidents, immediately report such information to the person responsible for the promotion of product security, the Product Security General Manager of the relevant product, and the LAS-IRT office in accordance with the LAS "Product Security Incident Response Guideline" (APQ-MQ-003)  Divisions shall stipulate auditing and self-check rules for ensuring that product security measures are taken appropriate, thus promoting improvement of operations.  The records related to these Operation Standards shall be kept in control in accordance with the “Quality Documents and Quality Records Control Standards” (APQ-BG-001).  These Standards shall come into force on April 1, 2022. | 2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2 |