|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **§ 543.20 - Information Technology and Information Technology Data** | |  |  |  |  |  |
| **(a)** | **Supervision** |  |  |  |  |  |
| 1. | Do controls identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(1) |  |
| 2. | Is the supervisory agent independent of the operation of Class II games? (Inquiry and review other – organizational chart) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(2) |  |
| 3. | Do controls ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(3) |  |
| 4. | Are information technology agents with access to Class II gaming systems prevented from having signatory authority over financial instruments and payout forms? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(4) |  |
| 5. | Are information technology agents with access to Class II gaming systems independent of and restricted from access to:  Financial instruments? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(4)  (i) |  |
| 6. | Are information technology agents with access to Class II gaming systems independent of and restricted from access to:  Accounting, audit, and ledger entries? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(4)  (ii) |  |
| 7. | Are information technology agents with access to Class II gaming systems independent of and restricted from access to:  Payout forms? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(a)(4)  (iii) |  |
| **(c)** | **Class II gaming systems’ logical and physical controls** |  |  |  |  |  |
| 8. | Are controls established and procedures implemented to ensure adequate:  Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(c)(1) |  |
| 9. | Are controls established and procedures implemented to ensure adequate:  Physical and logical protection of storage media and its contents, including recovery procedures? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(c)(2) |  |
| 10. | Are controls established and procedures implemented to ensure adequate:  Access credential control methods? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(c)(3) |  |
| 11. | Are controls established and procedures implemented to ensure adequate:  Record keeping and audit processes? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(c)(4) |  |
| 12. | Are controls established and procedures implemented to ensure adequate:  Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(c)(5) |  |
| **(d)** | **Physical security** |  |  |  |  |  |
| 13. | Is the information technology environment and infrastructure maintained in a secured physical location such that access is restricted to authorized agents only? (Inquiry and observation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(d)(1) |  |
| 14. | Are access devices to the systems’ secured physical location, such as keys, cards, or fobs, controlled by an independent agent? (Inquiry and observation)  (Definitional note: As used throughout this IT section, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for Class II gaming system, accounting, surveillance, essential phone system, and door access and warning systems.) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(d)(2) |  |
| 15. | Is access to the systems’ secured physical location restricted to agents in accordance with established policies and procedures, which includes maintaining and updating a record of agents, granted access privileges? (Inquiry, observation, and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(d)(3) |  |
| 16. | Is the network communication equipment physically secured from unauthorized access? (Inquiry and observation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(d)(4) |  |
| **(e)** | **Logical security** |  |  |  |  |  |
| 17. | Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:  Systems’ software and application programs? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(1)  (i) |  |
| 18. | Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:  Data associated with Class II gaming? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(1)  (ii) |  |
| 19. | Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:  Communications facilities, systems, and information transmissions associated with Class II gaming systems? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(1)  (iii) |  |
| 20. | Are unused services and non-essential ports disabled whenever possible? (Inquiry, observation and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(2) |  |
| 21. | Are procedures implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(3) |  |
| 22. | Are procedures implemented to ensure that all activity performed on systems is logged? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(3) |  |
| 23. | Are communications to and from systems via Network Communication Equipment logically secured from unauthorized access? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(e)(4) |  |
| **(f)** | **User controls** |  |  |  |  |  |
| 24. | Are systems, including application software, secured with passwords or other means for authorizing access? (Inquiry and perform log-in tests on network system(s) and each stand-alone system) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(1) |  |
| 25. | Is access to system functions assigned and controlled only by management personnel or agents independent of the department being controlled? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(2) |  |
| 26. | Does each user have his or her own individual access credential (such as passwords, PIN’s, or cards)? (Inquiry) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(3)  (i) |  |
| 27. | Are access credentials changed at an established interval approved by the TGRA? (Inquiry, review TGRA approval, and review other – system security settings) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(3)  (ii) |  |
| 28. | Are access credential records maintained for each user either manually or by systems that automatically record access changes and force access credential changes? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(3)  (iii) |  |
| 29. | Do access credential records include the following information for each user:  User’s name? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(3)  (iii)(A) |  |
| 30. | Do access credential records include the following information for each user:  Date the user was given access and/or password change? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(3)  (iii)(B) |  |
| 31. | Do access credential records include the following information for each user:  Description of the access rights assigned to user? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(3)  (iii)(C) |  |
| 32. | Are lost or compromised access credentials deactivated, secured or destroyed within an established time period approved by the TGRA? State the time period \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Inquiry and review TGRA approval) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(4) |  |
| 33. | Are access credentials of terminated users deactivated within an established time period approved by the TGRA? State the time period \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Inquiry and review TGRA approval) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(5) |  |
| 34. | Do only authorized agents have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts? (Inquiry and review other – authorization lists) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(f)(6) |  |
| **(g)** | **Installations and/or modifications** |  |  |  |  |  |
| 35. | Are only TGRA authorized or approved systems and modifications installed? (Inquiry and review TGRA approval) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(g)(1) |  |
| 36. | Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum:  The date of the installation or modification? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(g)(2)  (i) |  |
| 37. | Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum:  The nature of the installation or change such as new software, server repair, significant configuration modifications? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(g)(2)  (ii) |  |
| 38. | Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum:  Evidence of verification that the installation or the modifications are approved? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(g)(2)  (iii) |  |
| 39. | Are records kept of all new installations and/or modifications to Class II gaming systems that include, the following, at a minimum:  The identity of the agent(s) performing the installation/ modification? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(g)(2)  (iv) |  |
| 40. | Is documentation (such as manuals and user guides, describing the systems in use and the operation, including hardware) maintained? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(g)(3) |  |
| **(h)** | **Remote access** |  |  |  |  |  |
| 41. | Is documentation for each remote access system support session maintained at the place of authorization? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1) |  |
| 42. | Does documentation for each remote access session include:  Name of agent authorizing the access? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  (i) |  |
| 43. | Does documentation for each remote access session include:  Name of agent accessing the system? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  (ii) |  |
| 44. | Does documentation for each remote access session include:  Verification of the agent’s authorization? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  (iii) |  |
| 45. | Does documentation for each remote access session include:  Reason for remote access? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  (iv) |  |
| 46. | Does documentation for each remote access session include:  Description of work to be performed? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  ( v) |  |
| 47. | Does documentation for each remote access session include:  Date and time of start of end-user remote access session? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  (vi) |  |
| 48. | Does documentation for each remote access session include:  Date and time of conclusion of end-user remote access session? (Review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(1)  (vii) |  |
| 49. | Is all remote access performed via a secured method? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(h)(2) |  |
| **(i)** | **Incident monitoring and reporting** |  |  |  |  |  |
| 50. | Are procedures implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems? (Inquiry, review SICS, and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(i)(1) |  |
| 51. | Are all security incidents responded to within the established time period approved by the TGRA? State the time period\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Inquiry, review TGRA approval, and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(i)(2) |  |
| 52. | Are all security incidents and responses formally documented? (Inquiry, review TGRA approval, and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(i)(2) |  |
| **(j)** | **Data backups** |  |  |  |  |  |
| 53. | Do controls include adequate backup, including, but not limited to, the following:  Daily data backup of critical information technology systems? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(1)  (i) |  |
| 54. | Do controls include adequate backup, including, but not limited to, the following:  Data backup of critical programs or the ability to reinstall the exact programs as needed? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(1)  (ii) |  |
| 55. | Do controls include adequate backup, including, but not limited to, the following:  Secured storage of all backup data files and programs, or other adequate protection? (Inquiry and observation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(1)  (iii) |  |
| 56. | Do controls include adequate backup, including, but not limited to, the following:  Mirrored or redundant data source? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(1)  (iv) |  |
| 57. | Do controls include adequate backup, including, but not limited to, the following:  Redundant and/or backup hardware? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(1)  (v) |  |
| 58. | Do controls include recovery procedures , including, but not limited to, the following:  Data backup restoration? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(2)  (i) |  |
| 59. | Do controls include recovery procedures , including, but not limited to, the following:  Program restoration? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(2)  (ii) |  |
| 60. | Do controls include recovery procedures , including, but not limited to, the following:  Redundant or backup hardware restoration? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(2)  (iii) |  |
| 61. | Are recovery procedures tested on a sample basis at specified intervals (at least annually) and results documented? State the interval \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(3) |  |
| 62. | Are backup data files and recovery components managed with at least the same level of security and access controls as the system for which they are designed to support? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(j)(4) |  |
| **(k)** | **Software downloads** |  |  |  |  |  |
| 63. | Are downloads, either automatic or manual, performed in accordance with 25 CFR 547.12? (Inquiry and review SICS) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(k) |  |
| **(l)** | **Verifying downloads** |  |  |  |  |  |
| 64. | Following the download of any Class II gaming system software, does the Class II gaming system verify the downloaded software using a software signature verification method? (Inquiry and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(l) |  |
| 65. | Does the TGRA confirm the verification performed in checklist question 64 (TGRA can use any method it deems appropriate)? (Inquiry, review TGRA approval and review supporting documentation) | \_\_\_\_ | \_\_\_\_ | \_\_\_\_ | 543.20(l) |  |