| ផ្នែក  **តម្រូវការបច្ចេកទេសសម្រាប់ការរៀបចំមជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ អ.ស.ហ.** | តម្រូវការលម្អិត |
| --- | --- |
| ផ្នែកទី ១៖ ស្ថានភាពបច្ចុប្បន្ន |  |
| **១.១. បរិយាយអំពីប្រព័ន្ធដែលអង្គភាពសវនកម្មផ្ទៃក្នុងមាន៖**  **-ប្រព័ន្ធគ្រប់គ្រងរដ្ឋបាល និងបុគ្គលិក**  **-ប្រព័ន្ធរក្សាទុកទិន្នន័យក្លោដ**  **-ប្រព័ន្ធគ្រប់គ្រងការកក់បន្ទប់ប្រជុំ**  **-ប្រព័ន្ធរៀបចំរបាយការណ៍សវនកម្មឌីជីថល**  **-ប្រព័ន្ធស្នើសុំច្បាប់ឌីជីថល**  **-ប្រព័ន្ធគ្រប់គ្រងឯកសារចេញ-ចូល**  **-ប្រព័ន្ធវែបសាយ (គេហទំព័រ)** | * **រៀបរាប់ប្រព័ន្ធរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងកំពុងប្រើ​៖**   -ប្រព័ន្ធគ្រប់គ្រងរដ្ឋបាល និងបុគ្គលិក  -ប្រព័ន្ធរក្សាទុកទិន្នន័យក្លោដ  -ប្រព័ន្ធគ្រប់គ្រងការកក់បន្ទប់ប្រជុំ  -ប្រព័ន្ធរៀបចំរបាយការណ៍សវនកម្មឌីជីថល  -ប្រព័ន្ធស្នើសុំច្បាប់ឌីជីថល  -ប្រព័ន្ធគ្រប់គ្រងឯកសារចេញ-ចូល  -ប្រព័ន្ធវែបសាយ (គេហទំព័រ)   * **រៀបរាប់ប្រព័ន្ធរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងគ្រោងនឹងប្រើប្រាស់៖**   -ប្រព័ន្ធគ្រប់គ្រងការកត់ត្រាចំណូល/ចំណាយ  -ប្រព័ន្ធផ្តល់ទទួលទិន្នន័យរវាងអង្គភាពសវនកម្មផ្ទៃក្នុង និងអង្គភាពក្រោមឱវាទ **អ.ស.ហ.**  -ប្រព័ន្ធវិភាគទិន្នន័យសវនកម្មនៃការពិនិត្យឡើងវិញ |
| **១.២. បរិយាយអំពី​ Infrastructure**  ១.២.១. អង្គភាពសវនកម្មផ្ទៃក្នុងកំពុងប្រើប្រាស់ហេដ្ឋារចនាបណ្តាញរួមរបស់ អ.ស.ហ.  ១.២.២. Personal Server | * ចំនួន Server ១ សម្រាប់ប្រើប្រាស់លើការ Hosting Internal Applications |
| **១.៣.**  **ប្រព័ន្ធសុវត្ថិភាពរបស់អង្គភាពសវនកម្មផ្ទៃក្នុង**  ១.៣.១. បច្ចុប្បន្នអង្គភាពសវនកម្មផ្ទៃក្នុងប្រើប្រាស់ប្រព័ន្ធសុវត្ថិភាពរួមរបស់ អ.ស.ហ.  ១.៣.២. Clam Antivirus  ១.៣.៣. ប្រព័ន្ធទប់ស្តាត់ DDOS (Cloudflare) |  |
| ផ្នែកទី២៖ តម្រូវការលើប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន |  |
| **២.១. ពង្រឹងផ្នែកសុវត្ថិភាព**  ២.១.១. IPS/IDS  ២.១.២. Extended detection and response  ២.១.៣. Vulnerability Assessment  ២.១.៤. Web Application Firewall  ២.១.៥. Honeypot and Deception | * មូលហេតុនៃតម្រូវការផ្នែកពង្រឹងសុវត្ថិភាពនេះដើម្បីធានាសុវត្ថិភាពទិន្នន័យ និងការរំខានប្រតិបត្តិការលើបណ្តាញអ៊ីនធើណេត |
| **២.២. ព័ត៌មានសុវត្ថិភាព និងការគ្រប់គ្រងព្រឹត្តិការណ៍ (SIEM)**  ២.២.១. Platform Security  ២.២.២. Database  ២.២.៣. Application  ២.២.៤. Server |  |
| **២.៣. ការត្រួតពិនិត្យ​ និងតាមដាន**  ២.៣.១. តម្រូវការត្រួតពិនិត្យ​ និង តាមដានដោយផ្ទាល់​ និងពីរចំងាយ  ២.៣.២.​ មានក្រុមការងារដែលអាចត្រួតពិនិត្យ​ និងតាមដាន 24/7 |  |
| **២.៤. របាយការណ៍**  ២.៤.១. របាយការណ៍សុវត្ថិភាព  ២.៤.២. ប្រជុំរៀងរាល់មួយខែម្តងស្តីអំពីរបាយការណ៍សុវត្ថិភាព |  |