Risk Oheck

51

| | mehorizad are see falefination multimetion | 3- Middle | | | _ | Implement Rules | Implement Hulps: 135 Hulp Hone 7 |
|------------------|--|-------------|---|----------------|---|--|--|
| 52 2 Middle Ur | Unauthorized access, faisfination, malfunction Unauthorized access, faisfination, malfunction | 3: Middle | + | 2: Hugh (Spc) | - | | Implement Rules |
| | Unauthorized access, faisification, malfunction | 3: Middle | | 2: High (9pt) | 11 | Implement Rules | Implement Rules, GIS Rule Book |
| | Unauthorized access, faisification, malfunction | 3: Middle | | 2 High (9pt) | 1 | Implement Rules, | Implement Rulet, GIS Rule Book |
| 57 2. Middle Ur | Unsutherized access, faising abon, manunction Unsutherized access, faisification, maifunction | J: Middle | | 2 High (9pt) | 2: High (Spt) Implement Hule and Procedures. | | Implement Rule and Procedures. |
| | Unauthorized access, falsification, melfunction | 3: Middle | | 2: High (3pt) | | Implement Rule and Procedures. | Implement Rule and Procedures. GIS Ride Book |
| | Unauthorized access, falsification, melfunction | 3: Middle | | 2. High (Spt) | E I | Implement Rule and Procedures. CiS Ride Book | Implement Rule and Procedures. CIS Ride Book 2 |
| | Circuit breaker down | 3: Middle | | 2: High (9pt) | | Implement Rules. CIS Rule Book | Implement Rules. CIS Rule Book |
| | Information Itak | 3: Middle | | 2: High (Spd | | Implement Rules. | Implement Rules. GIS Rule Book 2 |
| B3 2: Middle Int | Information leak | 3: Middle | | 2 High (Spt.) | 2: High (3pt) Implement Rule and Procedures | | Implement Rule and Procedures |
| BS 2: Middle Ur | Unauthorized access, falsification, malfunction | 3: Middle | | 2: High (9pt) | 2: High (9pt.) Implement Rule and Procedures. | | Implement Rule and Procedures. |
| | Information leak | 3: Middle | | 2 High (Spt) | 1.1 | Implement Rules. | Implement Rules. GIS Rule Book |
| 68 2 Middle St | Staff errors to treat confidential information | 3: Middle | | 2 High (9pt) | 2 High (9pt) Implement Rules. | | Implement Rules. |
| | | | | | | | |
| 70 2 Middle Sc | Software Bay, matunction, maleare | 3. Middle | | 2: High (9pt) | 2: High (9pt) [Implement Rules. | E 1 | Implement Rules. GIS Rule Book |
| | Software Paw, mailunction, malware | 3: Middle | | 2: High (9pt) | L | Implement Rule and Procedures. | Implement Rule and Procedures. GIS Rule Book 2 |
| | Software Bar, malfunction, malware | 3: Middle | | 2: High (9pt) | Г | Implement Rule and Procedures. | Implement Rule and Procedures. CIS Rule Book |
| | Unuthorized access, falsification | 3: Middle | | 2 High (Spt) | Г | Implement Rules. | Implement Rules. GIS Rule Book |
| 2 Middle In | Information hais | 3: Middle | | 2 High (9p) | L . | Implement Rules. | Implement Rules. |
| | falsification | 3: Middle | | 2: High (9pt) | | Implement Rules. | Implement Rules. GIS Rule Book |
| | frace flag mail motion makers | 3. Michelle | | 2. High (0m) | | | |
| | Software flam maifunction, malware | 3: Middle | - | 2: High (Spit) | | | |
| L | finare flam, mailunction, maintine | | | 22 High (9p) | | | |

| ~ |
|----|
| 61 |
| π. |
| 5 |
| |
| £ |

| # Risk Evaluation | Comments on Threat | Vulnarabäty Comments on Valnarability | Total Risk Control Contents | 1.1 | References Threat Vulgarability |
|-------------------|---|---------------------------------------|-----------------------------|-----------------------|-------------------------------------|
| 130 | | | | | |
| 131 | | | | | |
| 132 2: Middle | Entry for external hadvers | 3: Middle | 2: High (Spt) | Implement Pules | |
| 133 2 Middle | Continuous unauthorized access | 3: Middle | 2: High (Spc) | | Implement Rules. GIS Rule Book |
| 134 2: Middle | Continuous unsuthorized access | 3: Middle | 2: H5(h) (Spt) | | Englement Rules. EIS Rule Beek 2 |
| 135 2: Middle | Circuit breaker down | 3: Middle | 2: High (5pc) | _ | Implement Rules. GIS Rule Book |
| 136 | | | | | |
| 137 2: Middle | Forced entry, unauthorized access | 3: Middle | 2. High (Spc) | Spc) Implement Rules. | _ |
| 138 2: M ddle | Forced entry, unauthorized access | 3: Middle | 2: High | | Enplement Rules. EIS Rule Book 2 |
| 139 2: N ddle | Forced entry, unauthorized access | 3: Middle | 2: High | | Implement Rules. GIS Rule Book 2 |
| 140 2: Middle | Forced entry, unauthorized access | 3. Middle | 2: High (9pc) | | Implement Rules. GIS Rule Book 2 |
| 141 2: N ddle | Unauthorized access, falsification mailunction | 3: Middle | 2: High (9pt) | - | Implement Rules. CIS Rule Book 2 |
| 142 2: M ddle | Unauthorized access, faisification, mailuneton | 3: Middle | 2: High (0oc) | | Implement Rules, CIS Rule Book |
| 143 2: M ddle | Staff errors to treat confidential information | 3: Midde | 2: High (Spc) | _ | Implement Rules, SIS Rule Book |
| 144 2: N ddie | Unsythonized access, falsification matunction | 3: Midde | 2: High (8pt) | - | Implement Rules. StS Rule Book 2 |
| 145 2: M ddie | Forced entry, unauthorized access | 3: Middle | 2: High (8pc) | | Implement Rules. SIS Rule Book |
| I46 2: M ddle | Data damage by software flaw and malfunction | 3: Middle | 2: High (9pt) | Implement Rules. | Implement Rules. GIS Rule Book |
| 147 2: M ddie | Forced entry, unauthorized access | 3: Middle | 2: High (Bp;) | | Implement Rules, SIS Rule Book |
| 148 2: M ddle | Service unavailable for a long time | 3: Middle | 2: High (Bpc) | _ | Implement Rules. |
| 149 2: M ddle | Continuous unauthorized access | 3: Middle | 2: High (9pc) | | Implement Rules. GIS Rule Book |
| 650 2: M ddja | Unauthonized access, falsification, mailunction | 3: Middle | 2: High (9p;) | | Implement Rules. GIS Rule Book 2 |
| 151 2: Middle | Unsuthonized access, faisification, mailunction | 3: Midda | 2: High (9pt) | - | Implement Rules. |
| 152 2: M ddle | Unauthorized access, falsification, mailunction | 3: Mi6de | 2: High (9pt) | _ | Implement Rules. GIS Rule Book 2 |
| 153 2: M ddle | Unsuborized access, felsification, mailunction | 3: Middle | 2: High (Bp;) | | Implement Rules. GIS Rule Book 2 |
| 154 2: M dole | Continuous unauthorized access | 3; Niddle | 2; Huth (9pc) | | Implement Rules. CIS Rule Book 2: |
| 155 2: Middle | Software flaw, mailune tion, maiware | 3: Middle | 2: High (9p3) | ⊢ | Implement Rules CIS Rule Book 2 |
| 156 2: Middle | Software flaw, malfunction, malware | 3: Middle | 2: High (Bpc) | 1 Implement Rules | Implement Rules. Cit's Rule Book 2 |
| 127 2: M ddle | Circuit breaker down | 3: Middle | 2: Huth (9m) | _ | _ |

| P | |
|-----------|--|
| ş | |
| <u>\$</u> | |

| - 07 | 184 | 183 | 182 | 18 | 180 | 179 | 178 | 177 | 176 | 175 | 174 | 173 | 172 | 17 | 170 | 169 | 168 | 167 | 165 | 165 | 164 | 163 | 162 | 6 | 160 | 159 | 158 | 4 | |
|----------------------|-------------------------------------|-------------------------------------|--------------------------------|---|---|--|---|--------------------------------|-------------------------------------|-----------------------------------|---|-----------------------------------|---|--|---|---|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----|----------------------|--------------------------------|--------------------------------|---|-----|-----|---------------------------|---------------------|
| | 84 Z: Niddle | 183 2: Middle | 182 2: Middle | 181 2: Middle | 80.2: Middle | 79 2: Middle | 78 2: Middle | 177 2 Middle | 2; Middle | 75 2: Middle | 74 2: Middle | 73 2: Middle | 72 2: Middle | 2: Middle | 70 2: Middle | 69 2: Middle | 68 2: Middle | 67 2: Middle | 65 2: Niddle | 65 2: Niddle | | 63 2: Niddle | 152 2: Niddle | IBI 2: Niddle | 2: Middle | | | Threat | Risk Evoluation |
| Circuit broader down | Software flaw, malfunction, malware | Software flew, malfunction, malware | Continuous unauthorized access | Unauthorized access, falsification, malfurction | Unjutherized access, falsification, malfunction | Unsutherized access, falsification, mail unotion | Unsutherized access, falsification, malfunction | Continuous unsutherized access | Service unavailable for a long time | Forced entry, unauthorized access | Data damage by software flave and malfunction | Forced entry, unauthorized access | Unsuthenized access, fidsification, malfunction | Staff errors to treat confidential information | Unsutherized access, falsification, malfunction | Unsutherized access, falsification, melfunction | Forced antry, unauthorized access | Forced antry, unauthorized access | Forced entry, unauthonized access | Forced antry, unauthorized access | | Circuit breaker down | Continuous unauthorized access | Continuous unsutherized access | Entry for external hackens | | | Comments on Threat | 00 |
| 3- Middle | 3: Middle | 3: Midde | 3: Nidde | 3: Middle | 3. Nidde | 3: Niddle | 3 Midde | 3: Nidde | 3 Nidde | 3: Nidde | 3: Nidde | 3 Midde | 3 Nidde | 3. Nidde | 3: Nidde | 3: Nidde | 3: Midde | 3: Middle | 3 Middle | 3: Middle | | 3: Midde | 3: Midde | 3: Midd e | 3. Midde | | | Vulnarability | |
| | | | | | | | | | | | | | | | | | - | | | | | | | | | | | Comments on Yulharability | |
| 2: High (12nd) | 2: High (12pt) | 2: High (13pc) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pd) | 2: High (12pd) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (13pt) | | | Total Risk | |
| | | | | | | | | | | | | | | | | | | | | | | | | | High (12pt) Suspended until PAIS integrating GAIS | | | Centrol Contents | Centrol |
| | | | | | | | | | | | | | | | | | | | | | | | | | LS I | | h | References | |
| 2 Middle | 2 Middle | 2 Niddle | 2 Niddle | 2 Niddle | 2: Niddle | 2: Niddle | 2: Niddle | 2: Niddle | 2. Niddle | 2 Niddle | 2: Niddle | 2: Niddle | 2: Niddle | 2: Niddle | 2 Niddle | 2: Niddle | 2: Niddle | 2: Niddle | 2 Niddle | 2: Niddle | | 2: Nidde | 2: Nidde | 2: Nixidia | 2: Niddle | | | Threat | Į, |
| 3. Viddle | 3: Vidde | 3: Viddle | 3. Vidde | 3: Middle | 3: Vidde | 3: Vidde | 3: Vidde | 3: Vidde | 3. Midde | J. Midde | 3: Midde | 3: Midde | 3: Midde | 3: Midde | 3: Middle | 3: Middle | J. Middle | 3: Middle | 3: Middle | J: Middle | | 3: Middle | J: Middle | 3. Middle | 3: Middle | | İ | Vunarability | ation after Centrol |
| 2: High (12) | 2; High (12) | 2: High (12pt) | 2: High (12p | 2: High (12p | 2: High (12p | 2: High (\$2p | (2: High (F2pt) | 2: High (12pt) | 2-High (T2p | 2: High (1:2pt) | 2: High (12pt) | 2: High (12p) | 2: High (12pt) | 2: High (12pt) | 2: High (H2pt) | 2 High (12p | 2: High (12pt) | Z: Migh (12pt) | 2 High (12pt) | 2 Nigh (12pt) | | 22 High (12pt) | 2: High (12pt) | 12 High (12)(2) | 22 High (12pt) | | ſ | Tetal Kusk | |

| <u>.</u> |
|----------|
| |
| 2 |
| 22 |
| 5 |
| 0 |
| |

| Theat | Commonts on Threat | Vyheretiky | Ocmmonts on Vulnerability | Total Risk | Control Contents | References | Threat |
|-----------------|---|----------------|---------------------------|---------------------|---|----------------------|----------------|
| | | | | | | | ++ |
| | | | | 1 - AD | | Pro Buile Barry | ÷ |
| 2: Middle | Farced entry, unauthonized access | 3. Modele | | 1 - Low (bot) | Define Rulas as implemented | GIS Rule Book | 27 Middle |
| BI 2 Middle P | Forced entry, unsuthorized access | 3 Middle | | 1: Low (0pt) | Define Rules as Implemented | GIS Rule Book | 27 |
| | Forced entry, unauthorized access | 3. Middle | | 1: Low (0pt) | Define Rules as Implemented | CIS Rule Book | 2: Middle |
| | Forced entry, unauthorized access | 3: Middle | | 2 High (19pt) | Implement Rules. | GIS Rule Book | 1 |
| 2: Middh | Information leas | 3: Middle | | 2: High (12pt) | Implement Rules. | GIS Rule Book | N MIGOL |
| 195 2 Midde 5 | Forced entry, unauthorized access | 3 Middle | | 2: High (15ot) | Implement Rules | GIS Rule Book | 2 Middle |
| | Forced entry, unauthorized access | 3: Middle | | 1:1.0m (0pt) | Define Rules as Implemented | GIS Rule Beck | Y |
| 2 Midde | Information leak | 余 Middle | | | Implement Rules | GIS Rule Book | 2. Middle |
| a lofe n | Encode action and activation of anomaly | 2 Michille | | 1. Low (Ont) | Implement Rules. | GIS Rule Book | ž |
| 2. Middle | Forest entry unsutherized access | 3: Middle | | 1: Low (0pt) | Implement Rules. | OFS Rule Book | 7: Niddia |
| 2. Migut | PORCES ENDY, UTBUDIDIZED ACCESS | Contraction of | | A 460 M 40 M | | | |
| | | | | The second | Online Bules as molemented | MS Rule Root | 2 Niddle |
| 2: Middle | Staff cross to uset considential information | 3. Maddle | | - Low (Doo) | Define Bules as incompoted | DIS Rule Book | 2 Niddle |
| 200 2: Middle 1 | Forced entry, unautronized access | A DECIM | | Low (0bc) | Define Rules as implemented | G(S Rule Book | 2 Niddle |
| | | | | | | | |
| 209 2: Middle 2 | Staff errors to treat confidential information | 3. Widdle | | | Implement Rules | GIS Rule Book | 2. 110 |
| 2: Middle | Forces entry, unauthorized access | 3- M (50% | | . 1. | Implement Policy. | Gie Buile Book | 2. Pridala |
| 212 Middle 1 | | | | and a second second | | | |
| | Insutheriand seconds. Intelligention multi-metion | 3- Mindala | | 1: Low (Ope) | Define Rules as Implemented | GIS Rule Book | 2: Niddle |
| 2 Wolds | Unauthorized access, faisification, mainmation | 3. Middle | | 2: High (12pt) | Implement Rules | GIS Rule Book | 2: Nidole |
| 2 Middle | Unauthorized access, faisfication matunation | 3 Middle | | 2. Math (12pt) | 2: Mah (12pt) Implement Bales. | CIS Rule Book | 2: Niddle |
| 2 Middle | Unautionized access, faisification, methanolog | 3- Middle | | 2: Migh (12pt) | Implement Rules, | GIS Rule Book | 2. N40 |
| 2 Middle | Unauthorized access, falsification, methanelion | 3. Mininile | | 2: High (12pt) | 2: High (12pt) Implement Rule and Procedures. | GIS Rvie Book | 2: Maddit |
| | Unauthonized access, falsification, mailunction | J- Middle | | 1: Low (opt) | | CITS Kule Boox | |
| | Unsuthenized access, fais/feation, maifunction | 3. Middle | | 1: Low (Jpt) | Calina Mules as implemented | CIS Bula Book | 2 Middle |
| 2. March | Characterization access, reservinger, manufactory | - Ministra | | 2. High (12nd) | 2. Mart (12nd) (molected), and ever requirements | CIS Rula Benk | 2 Midde |
| 223 2: Widdle | Information leak | 3. Middle | | 2: High (12pt) | | GtS Rule Book | 2. Middle |
| | ada mana ing Tang | T- Mindalia | | 2 High (Bent) | | CIIS Rule Book | 2 Midd |
| 9 2: Micole | Information leas | 4. MICOIR | | C. FIND YEAR | unifications round and in rounding str | 200 0 000 0 000 | and the second |
| 227 2 Middle | Unauthorized access, faisification, malfunction | 3: Middle | | Z: High (Bot) | | GIS Rule Book | 2 Middle |
| 2: Middle | Information leak | 3: Middle | | 2: High (9pt) | implement Rules, | GIS Rule Beok | 2: Middle |
| 2 301 2: Middle | Staff errors to creat confidential information | 3: Widdle | | 2: High (9pt) | Implement Rules | GIS Rute Book | 2: Middle |
| | | | | | | | |
| 2: Middle | Software flaw, malfunction, malware | 3: Middle | | 2 High (Bot) | Implyment Rules | CIS Rule Book | 2 Middle |
| 2 Midde | Seftware flaw, malfunction, malwara | 3. Viddla | | Z. High (Bot) | Implement huie and Procedures | Lais Rule door | O MIC |
| 2: Middle | Schware flaw, malfunction, malmare | 3: Meddlo | | 2 High (9oU | Inglement Rule and Proceedings | ALC DUE DOCK | N MOON |
| L | Unauthorized access, felsification | 3: Middle | | 2 High (9ot) | Implement Rules, | CAS Rule Book | 2 Middle |
| 2: Middle | Information leak | 3. Michtin | | 2 High (990) | Inclement Hures | CHS INUIA DOOM | 2. 140 |
| | Tols neation | A Moore | | A THE PARTY AND | Implement Dule and Decendance | DIS Duis Book | o vidella |
| | SETURITY LAW MATURATION MARKED | BLOOM C | | 4. INC. 1011. | THE REAL PARTY OF THE PARTY OF | Card Lines County | |

56

| - |
|----------|
| |
| <u>a</u> |
| σ. |
| 0 |
| × |
| æ. |
| <u>a</u> |
| × |

| Risk Evaluation | 1 Threat | | 242 | 243 | 244 | 245 | 246 | 247 | 248 | 249 | 250 | 251 | 252 | 253 | 254 | 254 | 254 255 256 | 254 255 258 | 254 255 258 258 | 254 255 258 258 258 |
|-------------------------------|---|---------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-------------------|-------------------|--|---------------------------------|
| 21 | Comments on Threat | | | | | | | | | | | | | | | | | | an and a state of the second | |
| | Vulnarability | | | | | | | | | | | | | | | | | | | |
| | Vulnarability Comments on Vulnarability | | | | | | | | | | | | | | | | | | | |
| | Total Risk | | | | | | | | | | | | | | | | | | | |
| Centrol | Centrol Contents | | | | | | | | | | | | | | | | | | | |
| | References | Rule book or Risk assessm | | | | | | | | | | | | | | | | | | |
| Risk Evaluation after Control | | assessment plan | | | | | | | | | | | | | | | | | | |
| Control | Vyharabilty Total Risk | | | | | | | | | | | | | | | | | | _ | |

| | 3 | 2 | | | 308 | | 300 | SOF | 304 | 303 | | | | 297 | | | | | | 30 | | 298 | | 285 | 285 | 284 | 282 | | | 278 | 277 | 272 | | M | 221 | | | | 266 | 265 | 261 | 262 | ľ | 1 |
|----------------|--------------------------------|------------------|------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--|-----|------------------|---|---------------------------------|------------------------------------|----------------------|---|---|--|---|---|--|---|--|---------------|----------------------|-----------------------------------|--|-----|------------------------------|--------------------------------------|---|-----------------------------------|----------------------------------|-------------------|-----------------------------------|-----------------------------------|---------------------------------|-----------------------------------|-----------------------------------|------------------------------------|-----------------------------------|-----------------------------------|-----|-----|-------------------------|--|
| | 2: Midda | 2: Middle | | 2: Midda | 2: Midde | 2: Midde | 306 Z: Midde | | 304 2: Middle | 2: Middle | 2: Middle | 2: MIDDIA | 2: Middle | | 1: Low | 1: Low | 2: Middle | 2: Middle | 2: Middle | 2: Middle | 2. Minimum | | 2: Middle | 2: Middle | 85 2: Middle | | 28312: Middle | 2. Minute | | 2: Middle | 2: Middle | 7 Mode | 2. Middle | 2: H | 400M 7 | 2 Model | 2: Middle | 2: Middle | 66 2: Middle | Low | | | Incost. | Theast |
| | filefication | Information lass | Unauthorized access. faisification | Software flaw, malfunction, malware | Software flaw, malfunction, malware | Software flaw, malfunction, malware | Staff errors to troot confidential information | | Information leak | Unsythemized access, fate-fleation, malfunction | Information leak | information and | Circuit breaker down | Unauthorized access, fait/fication, mailunction | Unauthorized access, fabrification, mailungtion | Unauthorized access, fabilitation, malfunction | Unauthorized access, fabilitation methodion | Unauthorized access, fabrification, molfunction | Unauthorized access, faisification, matunction | Unauthorized access, faisification, mathemation | Insufficient second fabilitation mathemation | | Information leak | Forced entry, unauthorized access | Staff errors to treat confidential information | | Information lead | Show ad approx an authorized appress | Configuration and total and shareful before and | Forced entry, snauthorized eccess | Forced ontry unauthorized access | Internation leas | Forced entry, unauthorized access | Forced entry, unauthorized access | Internation least | Forced entry, unautionized access | Forced entry, unauthonized access | Forces entry, unputhorized accests | Forced entry, unauthorized access | Forced entry, unauthorized access | | | Conversion Invest | |
| | 4 Hat | 3 Middle | 3: Middle | 3: Middle | 3: Middle | 3. Middle | C. MIDDle | | 3: Middle | 3 Middle | 3 Middle | 0.04000 | 3. Middla | 3: Middle | 3. Middle | 3. Middle | 3; Middle | 3. Niddle | 3: Middle | 3 Middle | 3 15-416 | | 3: Middle | 3: Middle | 3: Middle | | 3 Middle | 3 Middah | 9. UCLAR. | 3 Middle | 3: Nickdle | ADDIN 37 | 3. Middle | 4: Nigh | OCDIM (O | O NICOLO | 20 MICON | 2 Fair | 3. Middle | 2 Fair | | | Attraction | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Common (S on Yunatabuty | |
| 9. Li-L (00-+) | 2: Hah (16pt) | 2: Heh (12nt) | 2: Heh (15pt) | 2: Hah (12pt) | 2: High (12pt) | 2: Hah (12pt) | 002() 48H .2 | | 2: Hgh (12pt) | 2: Hah (12pl) | 2- High (12 M) | 00000 | 2. Hat (1204) | 2- 4145 (1250) | 1. Cow (0pt) | 1: Lew (Opt) | 2: Huth (12pt) | 1: Low (Opt) | 1: Low (0pt) | 2- High (32 pt) | 2- Hat (12n1) | | 2: Hah (\$2pt) | 2. Hat (12n) | 2: Hab (22nt) | | 2 Hab (12pt) | 2. 1441 (22.01) | 9 44 6 (1941) | 2: High (f2pt) | 2- High (12ot) | 2 1020 0200 | Z Han (1200) | 2: High (20pt) | A COMPANY AND A COMPANY | | 2 DED 1 200 | 1: Low (Opt) | 2: Hat (12pt) | 1: Law (Opt) | | | A OCT FRISK | |
| | 2: High (16pt) Implement Rules | Implement Rules | | | | Inglement Rules. | implement Kules, | | | Implement Rule and Precedures. | Instignant Rule and Precedures. | strage of the project of the state | Inglement, Rules, | Indianane, Rule and Precedules. | Define Rules as implemented | Define Rules as implemented | Implement, Rule and Procedures. | Implement, Rules, | Implement Rules. | Implement Rules | Datine Bulas as implementant | | | | Implement Rules | | Define Rules as implemented. | | Defens Drives as (mentamonial | Implement Rules. | | Interement rules. | Define Kules as implemented | Implement Rules. | a share as a share of the state | | | | Define Rules as implemented | Define Rules as implemented | | | Gourd Contents | |
| | GIS Fule Book | GIS Pule Book | GIS Fule Book | GIS Fula Book | GIS Ruin Book | GIS Rula Book | WE HUR BOOK | | GIS Fule Book | GIS Hule Book | GIS Rule Book | YOOD BILL CM | OKS Rule Book | CIS Pula Book | GLS Rule Book | GIS Hule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Ruie Book | İ | GIS Rule Book | GIS Rule Book | GIS Rule Book | | QIS Rule Book | GIS Rula Book | DIC DUC BOOL | GIS Rule Book | GIS Aute Book | ULO MUIS DOOM | GIS HU'E DOOR | GIS Fluie Book | | | | CIS Hule Book | OIS Fule Book | GIS Flute Book | | | National and a | The second second second second second second second second second second second second second second second se |
| 2 L.A.F. | 2: Middle | 2: Middle | 2: Middle | 2: Middle | 2: Middle | 2: Middle | Z. Mode | | 2: Middle | 2: Middle | 2: Middle | 7: 10:00 B | Z: Middle | 2: Middle | 2. Middle | 2: Middle | 2: Middle | 2: Middle | 2: Middle | 2: Middle | 2: Middle | t | 2. Middle | 2: Middle | 2: Middle | | 2 Middle | 2 Middle | 9. LAAA | 2: Middle | 2: Middle | aroun 7 | 2: Middle | 2: Middle | A. TOWN | A. MILLION | 2 M 000 | 2: Middle | 2 Middle | 2: M.ddla | | t | 1012 | |
| | 1: Low | | 1:Low | 1:10* | 1:Low | 1:Law | Lew | | Low | 1:10* | 1:Low | | WD-1 | 1:Law | 1:Low | 1: Low | 1: Low | 1:Low | 1: Low | 1: Low | 1. 0. | $\frac{1}{2}$ | 1: Low | 1: Low | 1:Low | | 1:Low | Low | 1-1-2-2 | 1: Low | 1: Low | I: LOW | NOT . | 1- Low | | 1 | 1.07 | Wey | Low | 1: Low | | | A NUMBER OF A | A DESCRIPTION OF A DESC |
| F- I are (day) | 1: Low (4pt) | 1: Low (4at) | 1: Low (4pt) | 1: Low (4pt) | 1: Low (4pt) | 1: Low (4pt) | LU MOX (490) | | 1: Low (4pt) | 1: Low (4al) | 1: Law (4ar) | Total and C | 1: Law (4pt) | 1: Low (dot) | 1: Low (0pt) | 1: Low (0pt) | 1: Low (Apr) | 1: Low (Opt) | 1: Law (0pt) | 1 Low (4pt) | 1: Low (4ot) | | 1: Low (4pt) | 1: Low (4pt) | 1: Low (4pt) | | 1: Low (4pt) | 1: Law (4at) | 1-1 Am (4A) | 1: Low (4pt) | 1: Law (4pt) | 10061 MO T 1 | 1 Low (10) | 1: Low (4pt) | Arth and a | T-Low (Apr) | A DEAL AND A | 1: Low (Up) | 1- Low (4pt) | 1- Low (0pt) | | t | 10.00 | |

58

| 1031 | 386 | 365 | 364 | 362 3 | 382 | 190 | | 100 | - | | 365 | | - | 353 | 1000 | 144 | | 347 | 348 2 | 345 | 344 | 343 | 342 | 341 | 240 | 200 | 195 | 336 | 305 | 334 | 333 | 221 | 330 | 329 | | | 326 | 323 | 322 | 321 | 320 | 315 | 318 | 310 | 315 | | |
|---|----------------------------------|------------------|------------------------------------|-------------------------------------|-------------------------------------|------------------------------------|--|---|--|--|-----|---|--|------------------|--|---|--|---|--|--|---|---|-----|-----|------------------|--|---|-----------------------------|-----------------------------------|--|-----|----------------------------------|-----------------------------------|-----|------------------|-----------------------------------|-----------------------------------|----------------------------------|-------------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----|-----|----------------------------|--|
| | 166 2 Niddle | 365 2 Middle | 64 3: + gh | 2: Middle | 382 1: Low | 1: Low | | 2. Mid-fla | 2 10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | 2 Middle | | 2: Niddle | | 2 Widdle | COLT NUCL | L OW | 1. LOW | 2: Middle | 2: Niddlo | 345 2: Middle | 2: Niddle | 2. Niddle | | | 340 2 Middle | A REAL | 2 15 1 - 16 | 3: 1: gh | 2 High | 3: Figh | | 2: M 000 | 2 Niddle | | 28 2 Middle | 2: Niddlo | 31.84 | 2: Niddlo | 2. Niddle | 2 Middlo | 325 2: Ni ddlo | 2 Niddle | 2 Middle | | | Bisk Evoluation | |
| Software from mailtanetics makers | faisification | anformation loak | Unautionized access, faisification | Software flaw, mailunction, malware | Software flaw, maifunction, malware | Software Ray, malfunction, malware | Locase under address much beaution are us assure | Staff among to the start confidential information | unterm au din teas. | Unsubjorized access, faisfication, mailunction | | information look | and the second second second second second second second second second second second second second second second | information leak | Chapter of the second state and the second state of the second sta | Unautronized access, faithfication, mathemation | Unsuborized access, faisfloation, evaluation | Unautionized access, faisification, mailunction | Unstationized access, faisification, macfunction | Unauthorized access, faisification, and function | Unautionized access, faisification, maifunction | Unauthorized access, faisification, mathunction | | | information lask | From and particle of the state | Staff arrest in Task confidential information | Information leak | Forced entry, unauthorized access | Staff arrens to treat confidential information | | r groed only, unsurranced access | Forced entry, unsultighted access | | information leak | Forced entry, unauthorized access | Forced entry, unauthorized access | inform stipp leak | Forced entry, uniquitionized access | Forced entry, unauthorized access | Forced entry, unsuthorized access | Forced entry, unauthorized access | Forced antry unsul havined access | | | Comments on Threat | |
| e Hoh | 4 High | S: Middle | 1: Middle | Middle | Far | S Fair | A CONTACT OF | C Middle | × 10000 | S Middle | | X Middle | 1.000.4 | S Middle | A MORE A | 10.000 | 1. 1. 1. | 3 Middle | 27 Middle | 3 Middle | S Middle | D Fair | | - | * Middle | d. Michael | C Modella | 4: High | 4: High | © Middle | | E rar | 3 Middle | | 2 Middle | % Middle | 4 High | S: Middle | 3 Middle | 3 Middle | 2 Fair | 2 Middle | 2 | | | Vulnarability | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | v Comments on Vulnarsbarry | |
| 2: High (2004) | 2: High (16pt) | | Z: High (10pt) | 2: High (12pt) | 1: Low (Opt) | 1: ow (Dpt) | | 2 High (12wh) | 0421/ uSH :2 | 2: tigh (12pl) | | 2; High (12pt) | ALC: NOT THE REAL PROPERTY OF | 2 - figh (12ab) | Coloris and a coloris | (1) WOLLS | 1.001 0001 | Z: -6mh (12m) | 2: High (12pt) | 2: Hgh(12pt) | 2: 4(gh (1201) | 2: -8xh (8pt) | | | 2: High (12ct) | A DESCRIPTION OF A DESC | 2: - Hah (12m) | 2: High (20pt) | Z: -6gh (20gt) | 1: _ow (0pt) | | 1.001 402 | Z: High (1200) | | Z: High (12pt) | 2: High (12pt) | 2: Hgh (2090) | 2: High (12pt) | 2: High (12pt) | 1: Low (Opt) | 1: Low (0pt) | 2: High (12oc) | 1: Low (Dot) | | | Total Risk | |
| 7 High (20xb) [Involution Paula and Provide and and Provide and Provide Action Paula and Provide Action Paula and Provide Action Paula and Provide Action Paula and | 2: High (16pt) (Implement Rules. | Inglement Rules. | Implement Rules. | Inplement Rule and Procedures. | Implement Rule and Procedures | Implement Rules. | A PRIME REPORTED | Frankers and Bulley | Indent Rules. | | | 2: figh (12pk) Implement Rule and Procedures. | | Inclement Rules | Increases note and a receipted | Define Hules as implemented. | Denne Hules at Inglemented | 2: High (12pt) Implement Rule and Procedures | Inplanent Bules | | Inplanent Roles. | Defene Rules as Implemented | | | Includent Fulse | | | Define Rules at Implemented | Define Rules as Implemented | Defere Rules as Inclemented | | | Copie ne nt. Bules. | | Implement Rules. | Define Rules as Implemented | Z: Hah (2000) (mplement Hules, | 2. High (12pc) [Implement Rules. | 2: High (12pt) [Implement Rules. | Define Rules at Implemented | Define Rules as Implemented | Define Rules at Implemented. | Define Rules at Inclemented | | | Control Contents | |
| CHS Rule Pront | GIS Rule Book | GIS Rule Book | GIS Rule Boot | GIS Rule Book | GIS Rule Book | GIS Rule Book | 2000 allo 1000 | DIS Bula Rash | CITIO HUNG BODS | GIS Rule Beek | | GIS Rule Beek | And the state | GIS Rule Book | CIC D. Is David | | CHS Pure Deex | GIS Rule Book | GIS Rule Beek | GIS Rule Beek | GIS Rule Book | GIS Rule Beek | | | GIS Rule Book | DIS Dula Bank | GIS Pule Bank | GIS Rule Book | GIS Rule Book | GIS Rule Book | | VIO DUN DIN | GIS Rute Book | | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | | | Raferences | |
| 2. Nutrin | 2: Middle | 2. Niddle | 2: Neddle | 2: Middlo | 2: Middle | 2: Niddla | Province 1 | 2. Niel-0a | DIDDeN 2 | 2 Middle | | 2: Niddlo | | 2. Niddla | A. MILLAR | 2: NHODIA | Z: Meddle | 2: Neddla | 2: Niddle | 2: Middle | 2: Middle | 2. Middle | | | 2: Niddla | D. Middle | A REAL | 2: Middle | 2. Niddla | 2: Niddla | | 0.00m 7 | 2: Maddle | | 2: Niddle | 2: Middla | Z: Meddie | 2: Meddle | 2: Middle | 2 Middle | 2: Naddie | 2: Naddie | N. Middle | | | Threat | |
| | 1: Low | I: Low | 1: Low | 1: Low | I: Low | 1: Low | 1.000 | - | II: LOW | LiLow | | 1:Low | | 1.000 | | 1: LOW | No. | I: LOW | 1: Low | 1: Low | 1: ow | 1: Low | | | | 1.00 | - | - OW | I: Low | 1: Low | | 1: LOW | | | I:Low | OW | E: LOW | I. Low | | | | 1: Low | 1: Low | | | Phenot Vulnerability | |
| 1. June (dated) | 1: Low (dpt) | 1: Low (4pt) | F: Low (4pt) | 1: Low (4pt) | 1: Low (0pt) | t: Low (Bpt) | COMEN MAN | 1. And days | LI LOW CODU | 1: Low (dol) | | 1: Low (4pt) | THE REAL PROPERTY AND A | li Lou (det) | TON NOT | I: Low (up) | 1: LOW (001) | Low (dot) | 1: Low (4pt) | 1: Low (101) | 1: Low (4pt) | 1:10% (10) | | | T Low (dot) | 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1 | 1 Jone Edmit | I: Low (dpt) | 1: Low (4pt) | 1: Low (Ept) | | LICEN WALLS | The second | | 1: Low (dpt) | 1: Low (1pt) | T: Low (4pt) | 1: Low (4st) | 1: Low (dpt) | 1: Low (bpt) | 1: Low (0pt) | 1: Low (4pt) | I: Low (Dpt) | | | Total Risk | |

| 420 | | | | | | 413 | 410 | 409 2 | 408 | | | 10 | 403 | 402. | 401 | 400 | BSE | 397 | 396 | 395 | 394 | 392 | | 056 | 389 | 100 | | 385 | | | 38 | | 378 | 377 | | 374 | | 372 | 371 | 359 | 1 | * |
|--|--------------------|------------------------------------|-------------------------------------|--------------------------------------|-------------------------------------|---|------------------|---|---|------------------|--------------------------------|----------------------|---|---|--|---|--|--|--|-----|-------------------|----------------------------------|--|--|----------------------------|---|---|----------------------------------|-----------------------------------|-------------------|---|---------------------------------------|-----------------------------------|-------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----|-----------------------------|---------------------|
| - Webe | 1: Low | S PUCh | 2: Middle | 2: Middle | 2: Middle | 4 DODIN 17 | 410 2: Midde | 2: Middle | ALCONOMIC | 2: Middle | 2: MIGON | 404 2: Midda | 403 2: Middle | 402 1: Low | 401 1 1 ow | 400 1- Low | 1: LOW | 397 1: OW | Low | | 394 C MI236 | - ow | - LOW | | 389 2: Midde | 1- | | 1.044 | 1: Low | | 2 Midda | 9- Hint | 2: Midd e | Z- MICHIe | 2- Middle | 2: Middle | 2: Middle | 2: Middle | 2: Middle | | | Threat |
| Software flow multi-notion and ware | Palsification leax | Unautronized access, faisification | Software flaw, mattunction, maiware | Software flyw, mailunction, mailware | Software flaw, matfunction, malware | Sum (right to freat pointential information | Information leak | Unauthorized access, falsification, mail/unoton | | Information leak | Inforvation leas | Circuit breaker down | Unauthorized access, faisification, malfunction | Unauthorized access, faisification, melfunction | Unsucherized access fabilitation mathemation | Unauthorized screen faitification mathemation | Unauthorized access, fakification, melfunction | Unauthorized access, faisfication, malfunction | Unsutherized eccess, fabilitation, mathemation | | Information least | Forced entry, unauthenzed access | Staff errors to treat confidential information | | Information least | COLUMN TO UNAN COLUMN AND INTO THE OFFICE | Charles a more the transfer and the set of the first state of the set of the | rorceg entry, unauthorced access | Forced entry, unauthorized access | | Information leak | three as a plan a parallel and an and | Forced entry, insufficized access | Information leas | Forced entry, unauthorized access | Forced entry, unauthorized access | Forced entry, unauthorized access | Forced entry, unauthonized access | Forced entry, unauthonized access | | Contraction and internation | Comments on Threat |
| A. Head | 1: Low | 3: Middle | 3: Middle | 3. Middle | 3: Middle | 3 Mode | 3. Middle | 2 F | 0. 11000 | 3. 10.44 | 3: Middle | 3: Middle | J: Middle | 2: Feir | 2. From | 3.54 | 2: Fair | 2: Far | 2. Fur | | 3: M 3 0 6 | 1: Low | 2: Far | 0.000 C | 2. 1. 1. | S: Middle | | Z: Fair | 2. Fair | 0.11000 | 1. Mindra | 9. HE444 | 3: Midde | 3: Niddie | 3: Middle | 3: Middle | 3: Middle | 3: Middle | 3: Middia | | Anderenda | Videonblity |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | CONTRACTOR ON YOUR BRIDDING | |
| | 2 High (12pt) | 2 High (15ct) | 2 High (12ac) | 2 High (125t) | 2 High (12pt) | 2 High (12pt) | 2 H5mh (12pt) | L Low (0pt) | 0371) WILL 7 | 5 Link (1944) | 2 High (15et) | 2 High (15pt) | 2 High (15pt) | 1 Law (Opt) | | 1000 ACT 1 | 1. Low (Opt) | 1. Law (Opt) | 1: Law (9pt) | | 2 Huth (15pt) | 1: Low (0p;) | 1: Low (0p;) | Addition of the | 1: LOW (Up) | 2; High (12m2) | | 1: Low (0pt) | 1: Low (0pt) | 2 10 1 10 10 | | | 2 High (12pt) | 2 High (12pt) | 2 Hat (12pt) | 1: Low (Opt) | 1: Low (0pt) | I: Low (Opt) | 1: Low (0nl) | | Mit of the little | Total Dick |
| A LAND THE REPORT OF THE REPOR | implement Rules. | | | Implement Rule and Procedures. | Implement Rules | Implament Rules. | | Implement Rule and Procedures. | THE LIVES IN DISTRICT THE AND PROCESSING S. | 0 | 2 High (15et) Implement Rules. | | | Define Rules as Implemented | Defice D. Les and Procedures, | implement huies. | impigraent Rules. | Implement Rules, | Define Rules as Implemented. | | Implement Rules. | | mplement Rules | A TABLE AND A DESIGN AND A DESI | Conne rules as implemented | Oefine Rules as implemented | | Complement Rules | Implement Rules. | Industry Long and | High (13pt) Centre rolles as implemented. | | Implement Rules. | Implement, Rules, | | | Define Rivies as Implemented. | Dafine Rules as Implemented. | Define Balas as Inclemented | | Control Contents | Control Contracts |
| COLO MARK COLO | GIS Rule Book | GIS Rule Book | GIS Rule Book | GIS Rul+ Beek | GIS Rule Book | GIS Rule Begin | GIS Rule Book | GIS Rule Book | O 5 Mile Book | | GIS Ruin Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | DIS MUR BOOK | Cills Nulle Blook | GIS Rule Back | GIS Rule Back | GIS Rule Book | | GIS Rule Book | GIS Fure Book | GIS Rule Book | City Now Down | Cite D. L. Book | GIS Rule Book | | GIS Rule Book | GIS Rule Book | MOD BOU ON | CHO BULL BOOK | 2 | CIS Rule Book | GIS Rule Book | CIIS Fluie Book | CIS Rule Book | GIS Rule Book | GIS Rule Book | CIS A.J. Bark | | renerances | Defenses |
| 1. 11 10 10 | 2 Niddo | 2: Midde | 2: Nidde | 2: Nidde | 2. Nidda | 2: Midde | 2 Midde | 2 Midde | 2: N 00. | | 2: Midde | 2 Midde | 2 Midde | 2. Middle | 2 Midde | 2: Middle | 2: Midde | 2. Midde | 2: Midde | | 2: Midde | 2 Midde | 2: Widde | 2 MILLS | 2: Middle | 2: Middle | | 2: Middle | 2: Middle | e o Celar | 2. Mildie | | 2: Midde | 2: Midde | 2: Middle | 2: Middle | 2: Middle | 2 Middle | 2 Midda | | Incat | There |
| | Low | I: Low | I: Low | 1: Low | 1: Cow | I: Low | 1: Low | 1: Low | 1: Low | | 1: Low | 1 Low | 1 Low | 1 Low | I Low | Low | I. Love | 1: Low | 1 Law | | 1 Low | I. Low | I Low | Lon | Low | Low | | 1 Low | 1: Low | I. Cow | Low | | 1: Low | 1: Low | 1: Low | 1: Low | 1: Low | | | | Uninerativy | Thread Videombilieu |
| THAN MALL | 1: Low (4pt) | I: Low (4pt) | I: Low (4pt) | 1: Low (4pt) | I: Low (4pt) | I: Low (4pt) | I: Low (4pt) | I: Low (Dpt) | 1: Low (4pt) | | II: Low (Spt) | 1: Low (Spt) | I: Low (Sot) | the set (Dec) | Low (Opt | I: Low (Opt) | I: Low (| I: Low (Opt | 1: Low (0pt) | + | 1: Low (Sot) | 1: Low (0x) | 1: Low (0:4) | IT LOPY (NOL | 1: Low (Upt) | 1: Low (4ot) | | 1: Low (Opt) | 1: Low (Opt) | 12 LOW | I: Low (4pt) | | Lithan (dot) | 1: Low (4pt) | 1: Low (4:0) | E: Law (Ost) | I: Low (Cot) | 1: Low (Ort | - | H | TOTAL PUSK | |

60

| SAL 2 | 5612 | | | 2000 | 2 | 553 2 | 557 | 355 2 | 554 2 | | | 200 | + | | 547 2 | | | | | | 541 2 | | 539 | 2 100 | 2 506 | 2355 | 0.34 | 533 3 | 532 3 | 531 3 | 830 | 200 | 527 2 | 526 | 525 2 | 524 3 | 522 3 | | 520 2 | 510.2 | 518 2 | | 2 616 | 51 | 513 | | ſ |
|----------------------------------|--------------------------------|-----------------------|-----------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-----|--|------------------|---|--|------------------------------|--------------------|----------------------|---|---|--|--|--|---|---|---|-------|------------------------|---|---|--|--|-----------------------------------|--|-----|---------------------------------------|-----------------------------------|-----|--------------------------------|---|-----------------------------------|---|---------------------------------|-----------------------------------|-----------------------------------|---|--|----|-----|--------------------------|---|
| - Madul- | Middle | 2. Lindala | High | Middle | Middle | Middle | | Middle | 2: Middle | 2 · Widdle | 6. TROUG | - Mindala | HEDRA 12 | - Middle | 2. Viddle | - OW | 11.04 | Z: Middle | 2: Widdle | 2: Viddle | 2: Viddie | 2: Widd'e | | 2" VIDIO | 6-D01A-2 | 5 Midde | | 1 High | 3: -684 | 3: High | | A A A A A A A A A A A A A A A A A A A | 2: Widde | | 2: Vidda | 524 3Each | 522 3- High | | 2. Vidda | 19.2. Widda | 2 Vidda | 517 2- US44 | 2- Vidde | | | Theast. | The second second second second second second second second second second second second second second second se |
| Software faw malfanetion malware | falsef eactors | Information Inst | Unsutherized access faicification | Software flaw, mallunction, maiware | Software flaw, malfunction, malware | Software flaw, malfunction, malware | | Staff errors to treat confidential information | Information teak | Unautherized access, faisification, methanetion | And the second sec | Infrarration load | Internation Isas | Circuit breaker down | Unsutivertied access, fee inducion, methodologi | Unauthorized access, fastification, mailunction | Unauthorized access, fail frequen, mailunction | Unauthorized access, faisingation, mailynction | Unauthorized access, faisification, mailunguon | Unsutherized access, faisification, mailunction | Unauthorized ancess, faitification, mailungtion | Unautoprized access, faisification, malfunction | | Set over at loss te as | reroed entry, unauthonized access | Statt errors to prest contridential information | Carlie and an annual stand stand at the second stand | Information leak | Forced entry, unauthorized access | Staff errors to creat confidential information | | CONCERNENT DEBUGGINERS BALANCE | Forced uning, unauthorized access | | Information leave | Forced entry, unauthorized access | Forced anity, unauthorized access | | Information leave | Forced antry, unsuthorized access | Forced entry, unauthorized access | Encode and a second horizon and account | Forced entry, unauthorized access | | | Comments on Threes | |
| A Har | 3 M ddla | 2. Made | 3 Middle | 3: Middle | 3: Middle | 3: Module | | 3: Middle | | 3: Middle | Albertun D | 2 Widdle | 316450M 15 | 3: Middle | 3. Middle | 3: Middle | 3. Middle | 3: Middle | 3: Middle | 3: Middle | 3: Middle | 3. Middle | | S. MICON | or Michole | S. Middle | 2 Martin | 3: Middle | 3: Middle | 3 Middle | | or months | 3: Middle | | 3. Middle | 3: Middle | 3: Middle | | 3: Middle | 3: Middle | 3: Middle | 3. Middle | 3. Middle | | | Autostation | _ |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Comments on Vulnaraberty | in the set of the set |
| 2 High (1Ree) | 2: High (12pt) | 0. Link (12.4) | 2 Hab (15or) | 2: High (12oc) | 2: High (12pt) | 2: High (12pt) | | 2: High (12pt) | 2: High (12pe) | 2: High (12ob) | 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 2. High (12m) | 2 Fight () 2020 | 2: High (12pt) | 2 High (200 | 1: Lew (0=0) | 1- Lew (0at) | Z: High (12gC) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | 2: High (12pt) | | (2021) uliH 22 | 1: LOW USE | (Sec) 457 : 1 | | 2 High (15pt) | 2: High (15pt) | 2: High (15pt) | | 1. 1219 (191) | 2: High (1205) | | 2: High (12pt) | 2: High (15pt) | 2: High (15pt) | | 2: High (12pt) | 2: High (12pt) | 1: Lew (0or) | 1: Lew (Bot) | 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1 | | | Notes and | |
| | 2: High (12pt) Implement Rules | International Contact | 2: High (15or) Implement Rules | | Implement Rule and Procedures | 2: High (12pt) Implement Rules, | | 2: High (12pt) Implement Rules. | Implement Rules | 2: High (12pt) Involument Rule and Procedures | A PLACE A SUCCESSION OF THE ALL PLACED AND A | Indenies Side and Department | Implement, nuites, | Implement Pules | | Define Rules as implemented. | Dating Ruling as Implemented | Implement hale and Procedures. | Implement Fulse. | | | | 1 I I | Implement no mules. | | Implement Pules, | | 2 High (15pt) Define Rules as Implemented. | Datina Rules as implemented. | Define Rules as implemented. | | | 2: High (1205) Implement Syles | | 2: High (12pt) Implement Pules | 2: High (15pt) Define Rules as implemented. | 2: High (15pt) Implement Rules, | | 2: High (12pt) Implement Fudes. | Implement Rules | Define Rules as implemented. | | | | | Carlos Construct | Control Contract. |
| Ale D.A. Baak | CIS Rule Book | | GIS Rule Rook | GIS Rule Book | CIS Pule Book | OIS Pule Book | | GIS Rule Book | CIS Fule Book | CIS Rule Book | ACC MALE PAR | CIS Bula Bank | GIS MUIS BOOK | GIS Nule Book | CIS Hule Book | GIS Hule Book | CIN HUIA HOOK | GIS NULL BOOK | GIS Ryle Dook | GIS Rule Book | GIS Bule Book | GIS Rule Book | | NO BUS SU | ACC BURNER | All Build Book | MC D.J. Bast | GIS Rule Book | CIS Rula Book | CIS Rule Book | | NOT SALL ON | CIS Rula Book | | GIS Rule Book | CIS Rule Book | GIS Rule Book | | OIS Fulle Book | GIS Rule Book | GIS Rule Book | GIS Rule Book | US NJA BOOK | | | 1001010100 | |
| A 101-0- | 2: Middle | P. Linda | 7. Middle | 7: Middle | 2: Middle | 2: Middle | | 2: Middle | 7: Middle | 2 Middle | T. TOTAL | 7. Widela | SID0-W 12 | 2. Middle | 2: Middle | 2: Middle | 7: Middle | C Middle | 2: Filddig | 2: Middle | 2. Middle | 2: Middle | | 5:00:00 S | | 2: Middle | 9. A. J.H. | Z: Middle | 2: Middle | 2: Middle | | 1.00000 | 2: Middle | | 2: Middle | 2: Middla | Z: Middle | | 2: Middle | 2: Middle | 2: Middle | 2: Middle | 7. Middle | | | 16 BUL | |
| | Low | 1 AU | 1-Low | F: Low | 1: Low | T: Low | | 1: Low | 1: Low | 1- Low | 1. 1. 1. | 1-1.70 | 1. 1.01 | 1: Low | T LOW | T: Low | T LOW | 1 LOW | T: LOW | 1: Low | 1: Low | 1: Low | | L: LOW | 1.07 | Low | 1 | T: Low | 1: Low | 1: Low | | | 1. Low | | T: Low | 1: Low | 11 | ł | 1: Low | 1: Low | 1: Low | : Low | LDW | | | Alitice Jension A | "hand Understablished |
| | Low(4pt | I ALL AND | I nw 4nt | 1: Low (4pt) | 1: Low (4pt) | 1 Low (4pt) | | 1: Low (4pt) | I: Low (4pt) | 1: Low (4pt) | Ndeven - | 1 mm (Ant) | NUCLEAR COLOR | I: LOW (40% | TOM (40) | I Low Opt | E LOW (Up) | 1 Low (4pt | 1: Low (4pt) | 1: Low (4pt) | f: Low (4pt) | I: Low (4pt) | | 1. LOW (4DD | 1 | 1001 400 | | I. Len (det) | I: Low (4pt) | 1: Low (4pt) | | Additional of | Low (4pt | | 1: Low (4pt) | 1: Low (4pt) | 1: Low (4pt) | | 1: Low (Apt) | 1: Low (4p) | 1: Low (Oot | 1. Low (Oot | Total And | | | VIIII INDI | - |

61

SECTION 5 Government Information Security Rule

- Drafted by Yusuke Tanaka, JICA Expert. - Edited by ICT Security Management Technical Team (iSMTT).

1. Introduction

<u>The Government Information Security Rule Book (GIS Rule Book) at NiDA</u> is defined as NiDA implements the Government Information Security Management System (GISMS) under <u>Information Security Management System Policy</u> and the <u>Government Information Security Management Manual</u> (GISMS Manual).

2. Three Basic Rules to Secure Information

[Rule 1] Always consider whether you acquire, process or save confidential information. Do NOT expose information against any risks of leakage, falsification and inaccessibility.

[Rule 2] Lock up an office entrance, a cabinet and a desk drawer before walking away for any moment.

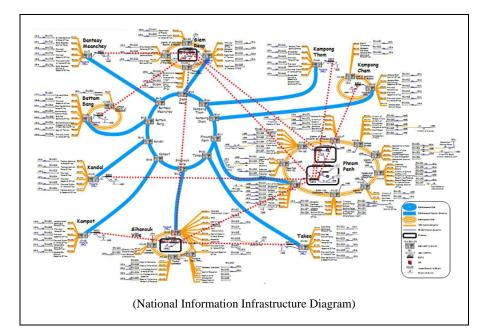
[Rule 3] Activate an auto-detection function of anti-virus software. Update a virus definition file at least weekly. Scan a storage device of your PC weekly and any external storage devices (e.g. FD, Memory Card/Stick and HDD) when to connect to your PC.

3. Scope

The GIS Rule Book covers National Information Communication Technology Development Authority (NiDA), which consists of the following departments; *General Administration, Infrastructure, Network, Enterprise, Content and Applications, Human Capacity Building and FOSS and Policy.* The GIS Rule Book also covers the following organizations under Secretary General; *Secretary General Office, Information Desk, Cambodia Computer Emergency Response Team, Singapore Operation Program, CISCO Training, and The Priority Management Group.*

From a network/system perspective, the GIS Rule Book covers client PC. The scope of GIS Rule Book will be extended to Servers and PAIS in the future.

NiDA has paid attention to develop the project Provincial Administration Information System (PAIS) and connect network system to all provinces.



4. Normative References, Terms and Definition

4.1. Normative References

The following referenced documents are indispensable for the application of this document.

1) <u>ISO/ISE 27001: 2005 Information technology – Security techniques –</u> <u>Information security management systems – Requirements</u>

2) <u>The Government Information Security Management System Manual</u> (GISMS Manual)

4.2. Terms and Definition

The followings are the terms and their definitions specifically used in GIS Rule Book.

Client PC:

It is a local PC as a type of desktop PC, laptop PC or mobile PC.

All other terms are referred to Terms and Definition in GISMS Manual or ISO/ISE 27001.

5. Information Security Organization

5.1. Information Security Organization Definition

NiDA sets the following information security roles and responsibilities.

Information Security Office (ISO):

It is set up at NiDA. It is responsible for implementing ISMS at NiDA. ISO members are CISO, IS Manager and IS In-charge, which are defined below.

Chief Information Security Officer (CISO):

One person is assigned at a ministry. He/she is also a member of Government Information Security Office (GISO), which is defined in GISMS.

Information Security Manager (IS Manager):

The role is assigned to an official by department. Its responsibilities are defined both in GISMS Manual and in GIS Rule Book.

Information Security In-charge (IS In-charge):

The role is assigned to an official also by department. Its responsibilities are defined in GIS Rule Book.

Official: All other employees of the in-scope organization.

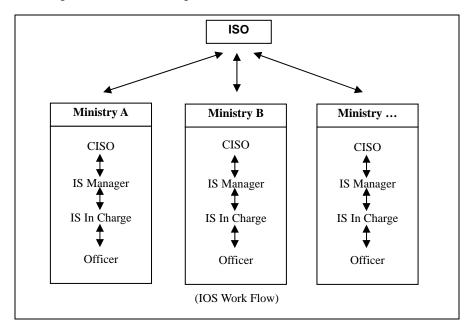
5.2. ISO Member List

ISO members will be assigned by the Secretary General of the National ICT Development Authority (NiDA).

5.3. Communication Route at Emergency

The reporting path is generally defined, from Officials to IS In-charge, IS Incharge to IS Manager, IS Manager to ISO/CISO. The instructing path is generally defined, from CISO/ISO to IS Manager, IS manager to IS In-charge, and IS Incharge to Officials in vice versa.

In the diagram is ISO work flow organization chart:



- 6. Rule and Procedures
 - 6.1. Information Classification

(a) Rule

- (a1) Information used in a government business operation is classified into three categories.
 - 1.General:
 - Open information which goes public
- 2.Internal:
- Information used only in a government business operation
- 3. Confidential:
- Confidential among limited authorized people
- (a2) Classify information when you acquire and it is highly recommended one is marked or labeled showing the information classification.
- (a3) Always manage information carefully according to the classification.
- (a4) Classify privacy information always as confidential.

(b) Procedure

(No procedure is applied for this section.)

6.2. People Security (To be defined in a future)

(a) Rule

(This section defines the security requirements of people matter such as the candidate qualification check in the hiring process, a job description related to information security matters, and the requirements at the termination of employment.)

6.3. Facility Security

6.3.1. Office Building and Room

- (a) Rule
 - (a1) Define those who can enter the facility/room.
 - (a2) Implement an appropriate key system for an entrance of the facility/room.
 - (a3) Separate an office space and the other accessible common space.
 - (a4) Get outsiders with an insider attendant.
 - (a5) Record an entry and exit.
 - (a6) Keep records of courier service.
 - Suspension
 - (b) Procedure
 - (No procedure is applied for this section.)

6.3.2. Cabinet and Desk

(a) Rule

(a1) Store information assets with confidential information and lock up cabinets.

(b) Procedure

- (No procedure is applied for this section.)
- 6.3.3. Fax Machine and Printer

(a) Rule

- (a1) Dispose printed materials/faxed materials with care.
- (a2) Keep record of faxing (sending/receiving).

(b) Procedure

(No procedure is applied for this section.)

6.4. Physical Information Security

6.4.1. <u>Paper</u> (a) Rule

- (a1) Always carefully identify confidential information within each paper/document.
- (a2) Save confidential paper/documents in safe against unauthorized access.
- (a3) Officials must burn disposing paper by themselves. Or use a paper shredder with disposing paper including confidential information.

(b) Procedure

(No procedure is applied for this section.)

6.4.2. Digital Archives (DVD/CD/FD/Tape)

(a) Rule

- (a1) Always carefully identify confidential information within each archive.
- (a2) Save confidential archives in safe against unauthorized access.
- (a3) Scrap a media (Tape/FD/CD/DVD) physically.
- (b) Procedure
 - (No procedure is applied for this section.)

6.5. Client PC Security

6.5.1. Desktop PC

(a) Rule Overall

(a1) The physical security of 'your' client PC is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.

(a2) All PCs MUST be assigned to a unique responsible official even if one is used by multiple officials.

(a3) You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. The password must be robust and be changed periodically. Never share it with anyone, not even members of your family, friends or IT staff.

(a4) Avoid leaving a PC unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

Virus Protection

(a5) Viruses are a major threat to NiDA and client PCs are particularly vulnerable if their anti-virus software is not kept up-to-date. The virus definition file MUST be updated at least weekly. The easiest way of doing this is simply to log on to the LAN for the automatic update process to run. If you cannot log on for some reason, contact Information Security Office

for advice on obtaining and installing anti-virus updates.

(a6) Always virus-scan any files downloaded to your computer from any source (FD/CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans must be set to happen automatically. It is also required to initiate scheduled scans at least weekly.

(a7) Report any information security events (such as virus infections) promptly to Information Security Office in order to minimize the damage.

(a8) Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting Information Security Office. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

(a9) Be especially careful to virus-scan your system before you send any files. This includes E-mail attachments and FD/CD/DVDs that you create.

(a10) Connect UPS for all desktop PCs not to lose information.

Disposal

(a11) Execute a physical formatting of storage in a PC not to leave any information readable.

(b) Procedure

For All Officials

Anti-virus Protection

(b1) The following procedure is defined to make sure that all PCs have the updated anti-virus software with a certain frequency.

| Step | Description | Owner | Records |
|------|--|--------------|------------------------------------|
| b1.1 | Instruct the submission of anti- virus software scan log. | ISO | n/a |
| b1.2 | Execute scan. | Official | n/a |
| b1.3 | Print out and submit a scan log. | Official | Anti-virus software scan log |
| b1.4 | File a scan log and keep for the defined period. | IS In-charge | n/a |
| b1.5 | Follow up those who has not executed a scan and submitted a log. | IS In-charge | n/a |

Virus Detection Handling

(b2) The following procedure is defined to take actions against virus

| Step | Description | Owner | Records |
|------|--|------------------|---|
| b2.1 | Detect an information security event such as virus detection. | Official | n/a |
| b2.2 | Physically off-line from a network immediately. | Official | n/a |
| b2.3 | Inform ISO immediately when the event happens. | Official | Information Security Event Report |
| b2.4 | Analyze the effects of an event and take an appropriate action. | ISO | n/a |
| b2.5 | Terminate any network/application services if necessary. | ISO | n/a |
| b2.6 | Execute an emergent anti- virus protection procedure if necessary. | ISO | n/a |
| b2.7 | Record an analysis and an action in a report. | ISO | (Updated) Information Security Event Report |
| b2.8 | File a report and keep for the defined period. | IS In- charge | n/a |

6.5.2. Laptop/Mobile PC

(a) Rule

Overall

The following rules are for laptop/mobile PC specifically. The laptop/mobile PC is also required to implement the rule and procedures defined in 6.5.1 **Desktop PC**.

(a1) Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

(a2) If you have to leave the PC temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.

(a3) Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.

(a4) Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about! Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

(a5) Government-owned laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.

(a6) Keep a note of the maker, model, serial number and the asset owner label (e.g. NiDA) of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform Information Security Office as soon as practicable (within hours not days, please).

Controls against unauthorized access to laptop/mobile PC data

(a7) Be highly recommended to use approved encryption software on all laptop/mobile PCs, choose a long, strong encryption password/phrase and keep it secure. Contact Information Security Office for further information on laptop encryption. If a laptop/mobile PC is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.

(a8) Do NOT save confidential information on your laptop/mobile PC instead of encrypting described in the previous clause.

(b) Procedure For All Officials

b1.4

Lost/Stolen Properties Event Handling

described as a normal information security event. Step Description Owner Records b1.1 Detect an information Official n/a security event such as a property lost or stolen. b1.2 Notify the Police. Official n/a b1.3 Inform ISO within an Official Information Security Event hour after the event happens. Report

ISO

(Updated)

Information

(b1) If a laptop/mobile PC is lost or stolen, follow the procedure

70

Analyze the effects of an

event and take an

| | | appropriate action. Record those in a report. | | Security Event Report |
|---|-----|---|------------------|--------------------------|
| b | 1.5 | File a report and keep it for the defined period. | IS In- charge | n/a |

6.5.3. Storage Devices (Portable Hard Disk / Memory Stick

/ Memory Card / Floppy Disk)

(a) Rule

Overall

(a1) Put an appropriate strap on those devices to keep them with you firmly. The recent high-tech storage devices are so small that they are easily dropped off and lost.

Virus Protection

(a2) Do NOT auto-run any storage devices when connecting to your computer.

(a3) Always virus-scan any storage devices when connecting to your computer.

Disposal

(a4) Execute a physical formatting of storage or scrap it physically not to leave any information readable.

(b) Procedure

For All Officials

Lost/Stolen Properties Event Handling

(b1) If any storage devices are lost or stolen, follow the procedure described in Lost/Stolen Properties Event Handling in Laptop/Mobile PC rule and procedures.

6.5.4. Personal Properties

(a) Rule

(a1) Get a permission of Information Security Manager to bring/take personal client PC related properties into/out of an office.

(b) Procedure

(No procedure is applied for this section.)

6.5.5. Software

(a) Rule

Overall

(a1) Install software explicitly allowed by IS manager.

(a2) Configure software according to IS In-charge instruction.

(a3) Apply patches promptly after IS In-charge instructs.

Unlicensed Software

(a4) Be careful about software licences. Most software, unless it is

specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and organizations are being prosecuted for infringing software copyright: do not risk bringing yourself and NiDA into disrepute by breaking the law.

Unauthorized Software

(a5) Do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the NiDA networks as well as affecting the working of your PC. Software packages that permit the computer to be 'remote controlled' (e.g. PCanywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on NiDA equipment properties unless they have been explicitly pre-authorized by management for legitimate business purposes. (e.g. Network Working Group for network auditing operation)

Backups

(a6) You must take your own backups of data on a client PC. The simplest way to do this is to logon and upload a data from the PC to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to FD/CD/DVD, USB hard disk /memory card/sticks etc. Make sure that off-line backups are encrypted and physically secured. Remember, if a client PC is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the PC. Off-line backups will save you a lot of heartache and extra work.

(b) Procedure

For Information Security Office

Patch Application Instruction

| Step | Description | Owner | Records |
|------|---|--------------|---|
| b1.1 | Update a standard software setting and the latest patches information list periodically. (The list may contains a general clause such as "Always apply windows update promptly unless it is prohibited explicitly.") | ISO | (Standard software setting and the latest patches information list) |
| b1.2 | Distribute the list to | IS In-charge | n/a |

(b1) The following procedure is defined to instruct apply patches.

| | Officials and enhance them apply promptly. | | |
|------|--|----------|-----|
| b1.3 | Apply patches promptly after IS In-charge instructs. | Official | n/a |

Software Setting Patrol Check

(b1) The following procedure is defined to audit software setting internally.

| Step | Description | Owner | Records |
|------|---|--------------|--|
| b1.1 | Plan and prepare software setting patrol check such as the date and sampled PCs. Instruct the setting before a patrol check. | ISO | n/a |
| b1.2 | Check software settings one by one. When found a nonconformance, instruct a PC owner fix the setting. | IS In-charge | n/a |
| b1.3 | Submit an Information Security Event Report if found a nonconformance. | Official | Information Security Event Report |
| b1.4 | File a report and keep it for the defined period. | IS In-charge | n/a |

6.5.6. <u>E-mail</u>

(a) Rule

(a1) E-mail attachments are now the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.

(a2) Do not use e-mail:

(a2.1) To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;

(a2.2) For private or charity work unconnected with the organization's legitimate business;

(a2.3) In ways that could be interpreted as representing or being official public statements on behalf of the organization, unless you are a spokesperson explicitly authorized by management to make such statements;

(a2.4) To send a message from anyone else's account or in their name (including the use of false 'From:' addresses). If authorized by the manager, a secretary may send e-mail on the manager's behalf but should sign the e-mail in their own name per pro ('for and on behalf of') the manager;

(a2.5) To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, color, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;

(a2.6) For any other illegal, unethical or unauthorized purpose.

(a3) Apply your professional discretion when using e-mail, for example abiding by the generally accepted rules of e-mail etiquette.

(a4) Review e-mails carefully before sending, especially formal communications with external parties.

(a5) Do not unnecessarily disclose potentially sensitive information in "out of office" messages.

(a6) Except when specifically authorized by management or where necessary for IT system administration purposes, officials must not intercept, divert, modify, delete, save or disclose e-mails.

(a7) Limited personal use of the corporate e-mail systems is permitted at the discretion of local management provided always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all e-mails traversing the government systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.

(a8) Be reasonable about the number and size of e-mails you send and save. Periodically clear out your mailbox, deleting old e-mails that are no longer required and filing messages that need to be kept under appropriate e-mail folders.

Suspension

(The clause will be activated after the government e-mail service installs the auto-scan function.)

(The clause will be activated after the government e-mail service gets stable.)

(b) Procedure For All Officials

Normal Information Security Events Handling

(b1) The following procedure is defined to report any information security events promptly.

| | Description | Owner | Records |
|------|---|------------------|--|
| Step | Description | Owner | Recolus |
| b1.1 | Detect an information security event such as undesirable/unsavory e-mails are delivered. | Official | n/a |
| b1.2 | Inform ISO within an hour after the event happens. | Official | Information Security Event Report |
| b1.3 | Analyze the effects of an event and take an appropriate action. Record those in a report. | ISO | (Updated) Information Security Event Report |
| b1.4 | File a report and keep it for the defined period. | IS In- charge | n/a |

6.5.7. Web Browsing

(a) Rule

Overall

(a1) Do not download an executable file without permission from Information Security Manager.

(a2) Download a file only which has a certification.

(a3) Do not click any links in an undesirable web site or e-mail.

(a4) It is highly recommended not to save cookies, which may cause User ID/password leak.

(a5) Set up a web browser associated to the previous clauses.

Inappropriate Materials

(a6) Be sensible! NiDA will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the client PC and steer clear of dubious websites. Information Security Office routinely monitors the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to Chief Information Security Officer, and disciplinary processes will be initiated. If you receive inappropriate material by e-mail or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call Information Security Office to check your spam settings.

(b) Procedure

For Information Security Office

Web Browser Setting Patrol Check

(b1) The following procedure is defined to audit web browser setting internally.

| Step | Description | Owner | Records |
|------|---|------------------|---|
| b1.1 | Plan and prepare web browser settings patrol check such as the date and sampled PCs. Instruct the setting before a patrol check. | ISO | n/a |
| b1.2 | Check web browser settings one by one. When found a nonconformance, instruct a PC owner fix the setting. | IS In- charge | n/a |
| b1.3 | Submit an Information Security Event Report if found a nonconformance. | Official | Information Security Event Report |
| b1.4 | File a report and keep it for the defined period. | IS In- charge | n/a |

6.6. Network and Server Security (To be fully defined in a future)

6.6.1. LAN and Internet

(a) Rule

Suspension

This section will be activated after PAIS is integrated with GAIS and system administration will be operated basically on PAIS. Develop a system administration manual for GAIS/PAIS and CamCERT network respectively which includes the updated network architecture/configuration and detailed operation procedures cooperating with other groups such as Information Security Office.

(b) Procedure

(No procedure is applied for this section.)

6.6.2. Server Common

(a) Rule

Suspension

This section will be activated after PAIS is integrated with GAIS and system administration will be operated basically on PAIS. Develop a system administration manual for GAIS and CamCERT system respectively which includes the updated system architecture/configuration and detailed operation procedures cooperating with other groups such as Information Security Office.

(b) Procedure

(No procedure is applied for this section.)

6.7. Application Software Security (To be defined in a future)

(a) Rule

(This section defines the information security requirements to application software and those to an application software development project.)

7. Information Security Training

7.1. Information Security Training Execution

All officials must get Information Security Training at least once a year. The following procedure is defined to plan and conduct information security training.

| | Description | Owner | Records |
|------|---|--------------|-----------------|
| b1.1 | Plan information security training both for the experienced and newly- hired officials | ISO | n/a |
| b1.2 | Conduct a training session. | IS In-charge | n/a |
| b1.3 | Record who took the session and keep it for the defined period. | IS In-charge | Training Record |

7.2. Promissory Letter Submission

All officials must once submit Promissory Letter to secure information. It is desirable to sign out at the time of training. The following procedure is defined to submit Promissory Letter.

| Step | Description | Owner | Records |
|------|--|--------------|-------------------|
| b2.1 | Distribute promissory letter blank. | ISO | n/a |
| b2.2 | Read through, sign out and submit one. | Official | Promissory Letter |
| b2.3 | File and keep it for the defined period. | IS In-charge | n/a |

8. Measurement

The following items will be measured by IS In-charge and reported at ISO at least yearly. The report enables to improve ISMS based on an objective detail.

| # | Measurement Name | Definition | Authorized by |
|---|---|---|---------------|
| 1 | Training Completion Rate | % of those who has completed training among all NiDA Officials | CISO |
| 2 | Information Security Event Mean Time to Process Completion by Event Type | Sum up (Process Completion Time - Event Occurred Time) divided by the number of events by Event Type* (Event Type is defined on an Information Security Event Report blank) | CISO |
| 3 | Anti-Virus Scan Execution Rate | % of those who has completed anti-virus scan among all NiDA Officials at the time of an anti- virus protection procedure issue. | CISO |
| 4 | Promissory Letter Submission Rate | % of those who has submitted Promissory Letter among all NiDA Officials | CISO |
| | -End of List- | | |

9. Breach (To be defined in a future)

(a) Rule

(This section defines the penalty against the information security breaches. It needs internal human resources regulation of government officials.)

10. Records List

| | | D C | D1 1 | A (1 * 1 |
|---|-------------|--------------------------------|------------|------------|
| # | Records | Reference | Blank | Authorized |
| | Name | | drafted by | by |
| 1 | Training | Chapter 7.1 Information | ISO | CISO |
| | Record | Security Training Execution | | |
| | | | | |
| 2 | Information | (1) Virus Detection Handling | ISO | CISO |
| | Security | Procedure in Chapter 6.5.1 | | |
| | Event | Desktop PC | | |
| | Report | (2) Lost/Stolen Properties | | |
| | | Handling Procedure in Chapter | | |
| | | 6.5.2 Laptop/Mobile PC | | |
| | | (3) Software Setting Patrol | | |
| | | Check Procedure in Chapter | | |
| | | 6.5.5 Software | | |
| | | (4) Normal Information Event | | |
| | | Handling Procedure in Chapter | | |
| | | 6.5.6 E-mail | | |
| | | (5) Web Browser Setting Patrol | | |
| | | Check Procedure in Chapter | | |
| | | 6.5.7 Web Browser | | |

| 3 | Anti-virus Software Scan Log | Anti-virus Protection Procedure in Chapter 6.5.1 Desktop PC | ISO | CISO |
|---|------------------------------------|--|-----|------|
| 4 | Promissory Letter | Chapter 7.2 Promissory Letter Submission | ISO | CISO |
| | -End of List- | | | |

SECTION 6 The Statement of Promise For Government Information Security

The Statement of Promise for Government Information Security

I hereby state the promise as follows, in order to keep government information secured as an official of Royal Governement of Cambodia.

- I am always compliant with Government Information Management System Policy, and with rules and procedures defined in Government Information Security Rule Book at the ministry I belong to.
- · I am responsible for that
 - It is always considered whether I acquire, process or save confidential information. I do not expose information against any risks of leakage, falsification and inaccessibility;
 - It is assured to lock up an office entrance, a cabinet and a desk drawer before walking away for any moment.
 - An auto-detection function of anti-virus software is activated. I update a virus definition file at least weekly. A storage device of my PC is scanned weekly and any external storage devices (e.g. FD, Memory Card/Stick and HDD) has to be also scanned when to connect to my PC.
- I fully understand the information security risks and the breaches of information security may be led to receive any penalties by authority.

| Signature | |
|-----------|---|
| (Title: |) |

Date _____

| 0 | |
|---|--|
| × | |
| | |
| _ | |