የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ

ጥቅምት 2014 ዓ.ም
አዲስ አበባ
ኢትዮጵያ

የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ

ጥቅምት 2014 ዓ.ም
አዲስ አበባ
ኢትዮጵያ

ማውጫ

ክፍል አንድ 1
1.1 መግቢያ 1
1.2 ዓላማ 1
1.3 ዝርዝር ዓላማዎች 2
1.4 የተፈፃሚነት ወሰን 2
1.5 መርሆች 2
1.6 የቃላት ፍቺ (ትርጓሜ) 3
1.7 የጸታ አገላለጽ 3
1.8 አህጽሮተ ቃላትና አጫጭር ስያሜዎች 3
ክፍል ሁለት፡ የሳይበር ደህንነት አደረጃጀት 4
2.1. ሚኒስቴር /ፕሬዝዳንት/ ዋና ዳይሬክተር/ሥራ አስፈጻሚ/ ሥራ አስኪያጅ/ 5
2.2. የሳይበር ደህንነት ዳይሬክቶሬት/ዋና ክፍል/ 6
2.3. የሳይበር ደህንነት መሪ (Steering) ኮሚቴ 8
2.4. የሳይበር ደህንነት አስተዳደር ቡድን (ክፍል) 9
2.5. የሳይበር ደህንነት ንቃተ ህሊና ቡድን (ክፍል) 11
2.6. የሳይበር ደህንነት ኢንጂነሪንግ ቡድን (ክፍል) 13
2.7. የሳይበር ደህንነት ኦዲት እና ግምገማ ቡድን (ክፍል) 15
2.2. የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ቡድን (ክፍል) 17
ክፍል ሶስት፡ የሳይበር ደህንነት አደረጃጀት የሥራ መደቦች 19
3.1. የሳይበር ደህንነት አስተዳደር ቡድን (ክፍል) የሥራ መደቦች 20
3.2. የሳይበር ደህንነት ንቃተ ህሊና ቡድን (ክፍል) የሥራ መደቦች 40
3.3. የሳይበር ደህንነት ኢንጂነሪንግ የሥራ ቡድን (ክፍል) መደቦች 63
3.4. የሳይበር ደህንነት ኦዲት እና ግምገማ ቡድን (ክፍል) የሥራ መደቦች 78
3.5. የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ቡድን (ክፍል) 96
ክፍል አራት፡ የማዕቀፉ አተገባበር 127
4.1. ማዕቀፉን ከተቋማት አውድ ጋር ስለማጣጣም 127
4.2. በማዕቀፉ አተገባበር ወቅት ትኩረት የሚሰጣቸው ጉዳዮች 128
4.3. ስለማዕቀፉ አተገባበር 128
4.4. የማዕቀፉ አለመፈጸም የሚያስከትለው ተጠያቂነት 129
4.5. ማዕቀፉን ስለማሻሻል 129
አባሪዎች 129

ክፍል አንድ

1.1 መግቢያ

አሁን ባለንበት ዘመን የተቋማትን መረጃዎች፣ የመረጃ መሰረተ-ልማቶችንና ስርዓቶችን ከሳይበር ስጋት፣ ተጋላጭነት እና ጥቃት መከላከል የሚያስችል አቅም መገንባት የተቋማትን ብሎም የሃገርን የሳይበር ደህንነት ራዕይና ተልዕኮ ለማሳካት አስፈላጊ ነው።

የሳይበር ደህንነት አቅም በተቋማት እና በሀገር ደረጃ ለመገንባት፤ እንዲሁም ከሳይበር ምህዳር የተገኙ እድሎችን ለመጠቀም እንዲያስችል የሳይበር ደህንነት አደረጃጀት መዘርጋት እና ለመዋቅሩ የሚመጥን እውቀትና ክህሎት ያላቸው አመራሮችንና ባለሙያዎችን መፍጠር የሳይበር ደህንነትን ለማረጋገጥ አስቻይ ሁኔታዎችን ይፈጥራል። አደረጃጀቱ እና የሥራ መደብ መዋቅሩ የሃገራችንን የሳይበር ደህንነት ራዕይና ተልዕኮዎች ለማሳካት መሰረታዊ ከሆኑ ጉዳዮች አንዱ በመሆኑ በሁሉም የመንግስትና ቁልፍ የግል ተቋማት ውስጥ ለመዘርጋት እንዲያስችል ሆኖ ተዘጋጅቷል።

ስለሆነም ሰነዱ የሳይበር ደህንነትን ለመምራትና ለማስተዳደር የሚያስችል የተቋማትን አውዳዊ ሁኔታ ባገናዘበ መልኩ በሁሉም የመንግስት እና የግል ቁልፍ ተቋማት ውስጥ የሚተገበር አደረጃጀት እና የሥራ መደብ መዋቅር የያዘ ነው።

በመሆኑም የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲን(ኢመደኤ) እንደገና ለማቋቋም በወጣው አዋጅ ቁጥር 808/2006 አንቀጽ 6 ንዑስ አንቀፅ 2 እና 3 በተሰጠው ስልጣን መሰረት ይህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ ሊዘጋጅ ችሏል።

1.2 ዓላማ

በሁሉም የመንግስት እና ቁልፍ የግል ተቋማት ውስጥ የሚገኙ መረጃዎችን፣ የመረጃ መሰረተ-ልማቶችንና ስርዓቶችን ከሳይበር ስጋት፣ ተጋላጭነት እና ጥቃት ለመከላከል፣ እንዲሁም የሳይበር ደህንነትን ለማረጋገጥ የሚያስችል የተቋማትንና የሀገርን አውድ ያገናዘበ አደረጃጀት እና የሥራ መደብ መዋቅር እንዲኖር ለማስቻል፤

1.3 ዝርዝር ዓላማዎች

ሀ. በተቋማት ደረጃ ግልጽ የሆነ የሳይበር ደህንነት የሥራ ድርሻ እና ኃላፊነትን ለይቶ ለማስቀመጥ፤

ለ. የተቋማትን መረጃዎች፣ የመረጃ መሰረተ ልማቶች እና የመረጃ ስርዓቶችን ደህንነት ለማረጋገጥ የሚያስችል ስርዓት እንዲኖር ለማስቻል፤

ሐ. ከሀገራዊ የሳይበር ደህንነት ፖሊሲ፣ ስትራቴጂዎች፣ ስታንዳርዶች እና ህጎች ጋር የተጣጣመ አደረጃጀት በተለያዩ ተቋማት እንዲኖር ለማድረግ፤

1.4 የተፈፃሚነት ወሰን

ይህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ በሃገሪቱ በሚገኙ በሁሉም የመንግስት እና ቁልፍ የግል ተቋማት ውስጥ የተቋማቱን ዓውድ ባገናዘበ ሁኔታ ተፈፃሚ ይሆናል፡፡

1.5 መርሆች

እነዚህን መርሆች እንደመነሻ በመጠቀም ተቋማት የራሳቸውን ተልዕኮና አውድ ባገናዘበ ሁኔታ ሌሎች መርሆችን ማካተት ይችላሉ፡፡ ይህ ማዕቀፍ የሚከተሉትን መርሆዎች ታሳቢ ያደርጋል፡፡

ሀ. ተጠያቂነት፡- ይህ ማዕቀፍ በሚተገበርባቸው ሁሉም ተቋማት ውስጥ በመዋቅሩ የተመደበ አመራርም ሆነ ባለሙያ የሚሰጣቸውን ተግባራት በተጠያቂነት ይፈጽማሉ፡፡

ለ. ኃላፊነት፡- በዚህ አደረጃጀት የሚመደቡ ኃላፊዎችና ባለሙያዎች የተሰጣቸውን ተግባርና ኃላፊነት በግልጽ የማወቅ፣ የመቆጣጠር፣ ሚናቸውን የመለየት እና የተጣለባቸውን ኃላፊነት በአግባቡ መወጣት ይኖርባቸዋል፡፡

ሐ. አውዳዊነት፡- ይህ ማዕቀፍ ውጤታማ እንዲሆንና የታለመለትን ዓላማ እንዲያሳካ የተቋማትን ራዕይና ተልዕኮ ባገናዘበ ሁኔታ ተፈፃሚ ይሆናል፡፡

መ. ቅንጅትና አጋርነት፡- የሳይበር ደህንነትን ማረጋገጥ የሁሉም ባለድርሻ አካላት ተሳትፎ የሚጠይቅ በመሆኑ ሁሉም በዚህ ማዕቀፍ የተጠቀሱ አደረጃጀቶች ከሌሎች የሚመለከታቸው ባለድርሻ አካላት ጋር በቅንጅትና በአጋርነት መስራት ይጠበቅባቸዋል፡፡

1.6 የቃላት ፍቺ (ትርጓሜ)

ቁልፍ የመረጃ መሰረተ-ልማት ማለት በሀገሪቱ ማህበራዊ፣ ኢኮኖሚያዊ እና ፖለቲካዊ ጥቅሞች ዙሪያ ከፍተኛ አስተዋጽኦ የሚያደርግ፤ በባህሪው ለሳይበር ጥቃትና ስጋት ተጋላጭ የሆነና በሚደርስበት ጥቃትም ከፍተኛ ጉዳት ሊያስከትል የሚችል መሰረተ ልማት ነው።

የመረጃ ስርዓት ማለት በተቋማት ውስጥ የሚገኙ መረጃዎችን ለማሰባሰብ፣ ለማደራጀት፣ ለማከማቸትና በተቀናጀ ሁኔታ በዕውቀት ለመጠቀም የሚያስችሉ ስርዓቶችን፣ እንዲሁም ስርዓቶቹን ለመምራትና ለማስተዳደር የሚያችል ገዢ ሰነዶችን (ፖሊሲዎች፣ ስትራቴጂዎች፣ ስታንደርዶች፣ ፕሮግራሞች፣...ወዘተ) ያካትታል።

የመወዳደሪያ አቅም ማለት አመራሩና ባለሙያው የተሰጣቸውን ኃላፊነትና ተግባር በአግባቡ ለመወጣት የሚያስፈልጋቸው ብቃት ነው።

የሳይበር ምህዳር ማለት እርስ በርሳቸው የተሳሰሩ መረጃዎች፣ የመረጃ መሰረተ ልማቶች፣ መረጃ ስርዓቶች፣ መረጃን ወደ እውቀት የሚቀይርና የሚጠቀም የሰው ሃይል፤ እንዲሁም ተቋማዊና ማህበረሰባዊ ባህል ያካተተ ምህዳር ነው።

ሳይበር ደህንነት ማለት በሳይበር ምህዳር የተፈጠሩ አስቻይ ስርዓቶችን ከተለያዩ የሳይበር ስጋቶች፣ተጋላጭነቶችና ጥቃቶች በመከላከል ሀብቶችን፣ የአሰራር ሂደቶችንና መዋቅሮችን በተደራጀና በተቀናጀ መልኩ መጠቀም ነው።

የሳይበር ጥቃት ማለት በሳይበር ምህዳር የሚፈጸም ያለፈቃድ ብርበራ፣ የመረጃ ስርቆት፣ ቫይረሶችን ማሰራጨት፣ ስነ ልቦናዊ ጦርነት እና ሌሎችም መሰል የሳይበር ጥቃቶችን ያካትታል።

የሳይበር ደህንነት ፖሊሲ ማለት የሳይበር ደህንነትን ለመምራት፣ ለማስተዳደርና ውሳኔ ለመስጠት የሚያስችል ሰነድ ነው።

1.7 የጾታ አገላለጽ

ማንኛውም በዚህ ማዕቀፍ በወንድ ጾታ የተገለጸው የሴትንም ጾታ ያካትታል፤

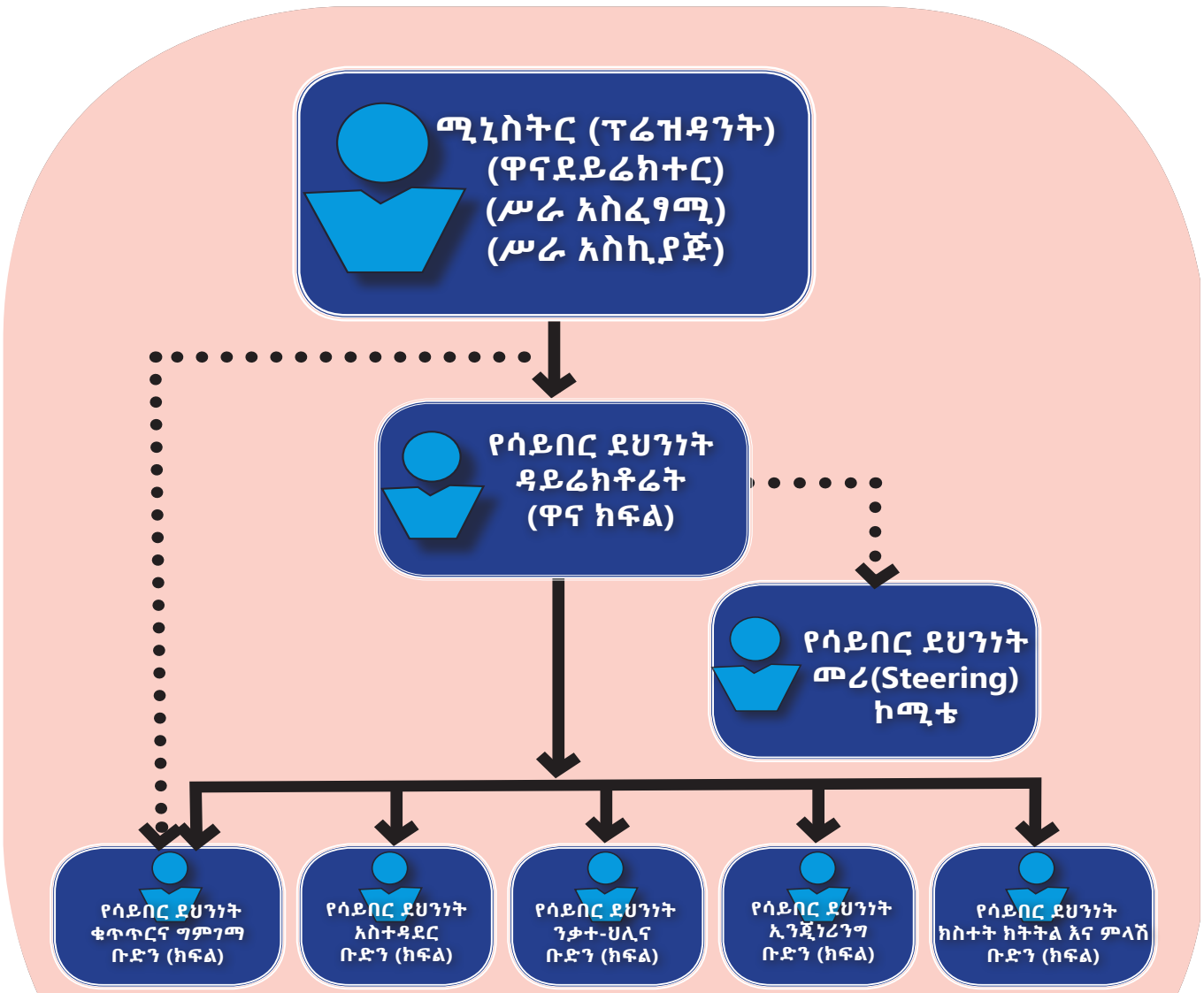
1.8 አህጽሮተ ቃላትና አጫጭር ስያሜዎች

ኢመደኤ፡ ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ

ኢኮቴ፡ ኢንፎርሜሽን ኮምዩኒኬሽን ቴክኖሎጂ

ክፍል ሁለት፡ የሳይበር ደህንነት አደረጃጀት

ይህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ በሃገር አቀፍ ደረጃ የተቋማትን አውድ ባገናዘበ ሁኔታ ተፈፃሚ የሚሆን ነው፡፡ አደረጃጀቱ ከሚኒስቴር/ፕሬዝዳንት/ዋና ዳይሬክተር/ሥራ አስፈጻሚ/ እስከ ባለሙያ ድረስ ያለውን የሚያካትት ሲሆን በየደረጃው የሚገኙ አደረጃጀቶች ተግባርና ኃላፊነት በግልፅ ለማስቀመጥ ተችሏል፡፡ በመሆኑም አደረጃጀቱ እንደአስፈላጊነቱ ተቋማት ከራሳቸው አውድ አንጻር በመመልከት ተግባራዊ ማድረግ የሚጠበቅባቸው ሲሆን እንደሚከተለው ተቀምጧል፡፡



ስዕል 0 1፡ የሳይበር ደህንነት አደረጃጀት

2.1. ሚኒስቴር /ፕሬዝዳንት/ ዋና ዳይሬክተር/ሥራ አስፈጻሚ/ ሥራ አስኪያጅ/

አጭር መግለጫ

የተቋሙን የሳይበር ደህንነት በበላይነት የሚመራ፣ የሚያስተዳድር፣ ከተቋሙ ተልዕኮ ጋር በተያያዙ ጉዳዮች ዙሪያ ስትራቴጂክ ዕይታዎችን በመከተል በኃላፊነት አቅጣጫ የሚያስቀምጥ አካል ነው። የሳይበር ደህንነት አደረጃጀት ዓላማውን እንዲያሳካ ክትትልና ድጋፍ በማድረግ፣ አቅም በመገንባት እና ውጤታማነትን በማረጋገጥ በሥሩ ካሉ ክፍሎች ጋር ይሰራል። እንዲሁም የሳይበር ደህንነትን አስመልክቶ የተቀረጹ አዳዲስ ፕሮግራሞችን ኃላፊነት በመውሰድ በጀት በመመደብ ተግባራዊ ያደርጋል። በመሆኑም ሚኒስትር/ፕሬዝዳት/ዋና ዳይሬክተር/ሥራ አስፈጻሚ/ሥራ አስኪያጅ/ የሚከተሉት ዋና ዋና ተግባሮችና እና ኃላፊነቶች ይኖሩታል።

ዋና ዋና ተግባሮችና ኃላፊነቶች

ሀ. የሳይበር ደህንነት ስትራቴጂክ ዕቅድ ዝግጅትን በበላይነት ይመራል፣ አፈጻጸሙን ይከታተላል፤

ለ. በተቋሙ የሳይበር ደህንነት አሰራር ስርዓት መዘርጋቱን ያረጋግጣል፤

ሐ. ሃገራዊ የሳይበር ደህንነት ፖሊሲ፣ ስትራቴጂዎች፣ ስታንዳርዶችና ሌሎች ህግጋት በተቋሙ መተግበራቸውን ያረጋግጣል፤

መ. የተቋሙን የሳይበር ደህንነት ፖሊሲ እና መመሪያዎች ውጤታማነት ያረጋግጣል፤

ሠ. የሳይበር ደህንነት መለኪያዎች መቀመጣቸውን ያረጋግጣል፤እንዲሁም በመለኪያዎቹ መሰረት እንዲከናወን አቅጣጫ ይሰጣል፤

ረ. የሳይበር ደህንነት ስቲሪንግ ኮሚቴን በበላይነት ይመራል፤

ሰ. የሳይበር ደህንነት ቁጥጥር /ኦዲት/ ሪፖርት በመገምገም አስፈላጊውን የማስተካከያ እርምጃ እንዲወሰድ አቅጣጫ ያስቀምጣል፤

ሸ. ዓመታዊ የሳይበር ደህንነት የሥራ ዕቅድና የአፈፃፀም ሪፖርት ለሚመለከታቸው የመንግስት አካላት ያቀርባል፤

2.2. የሳይበር ደህንነት ዳይሬክቶሬት/ዋና ክፍል/

አጭር መግለጫ

ይህ ዳይሬክቶሬት/ዋና ክፍል/ የተቋሙን የሳይበር ደህንነት የሚመራና የሚያስተዳድር የሥራ ክፍል ነው። የሳይበር ደህንነት መመሪያዎች እና ፕሮግራሞች መቅረጽና ማስተዳደር፣ እንዲሁም አዳዲስ አስተማማኝ የደህንነት መፍትሄዎችን ከማዘጋጀት ባሻገር የተቋሙን የሳይበር ደህንነት በአስተማማኝ መልኩ ማስተዳደር ነው። ዳይሬክቶሬቱ/ዋና ክፍሉ/ የተቋሙን የመረጃ ሃብቶች ምስጢራዊነት፣ ምልዑነት እና ተደራሽነት በሚመለከት ፖሊሲዎችንና ሂደቶችን የመምራት እና የማስተዳደር ኃላፊነት አለበት። በመሆኑም ዋና ዋና ተግባር እና ኃላፊነት በሚከተለው መልኩ የተዘረዘረ ሲሆን ሌሎች መስፈርቶች (ዕውቀት፣ ክህሎት፣ የትምህርት ደረጃ፣ ሰርተፍኬት እና የመወዳደሪያ አቅሞች ከዚህ ሰነድ ጋር አባሪ (ቅጽ 1 እና 2) ተደርገዋል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. የሳይበር ደህንነት ፖሊሲ ዝግጅትን ይመራል፤

ለ. ሃገራዊ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ መነሻ በማድረግ የተቋሙን የሳይበር ደህንነት አመራር ስርዓት ያጎለብታል፣ በየሁለት ዓመቱ እንዲከለስ ያደርጋል፣ ያስተዳድራል፤

ሐ. የሳይበር ደህንነት መመሪያዎችን እና አሰራሮችን /ፕሮሲጀሮችን/ ያፀድቃል፤

መ. የሳይበር የደህንነት ስትራቴጂዎችን እና ስርዓቶችን በማቀናጀት እንዲተገበሩ ያደርጋል፤

ሠ. የተቋሙን የሳይበር ደህንነት ፖሊሲዎችና ፕሮሲጀሮችን ውጤታማነት በየጊዜው ይፈትሻል፣ ይገመግማል፣ ያረጋግጣል፤

ረ. የሳይበር ደህንነት አመራር ስርዓት አፈጻጸምን ይገመግማል፤

ሰ. አዳዲስ የሳይበር ስጋቶችን እና ተጋላጭነቶችን ለመለየት የሚያስችል ዓመታዊ እና መደበኛ የሳይበር ደህንነት ክስተት ዳሰሳ (risk assessment) ያደርጋል፤ አዳዲስ ስጋቶችንና ተጋላጭነቶችን ለመቀነስ የሚያስችል እርምጃ ይወስዳል፤

ሸ. የመረጃ ስርዓቶች አገልግሎት ከመስጠታቸው በፊት የሳይበር ደህንነት ክፍተት ዳሰሳና ትንተና ውጤት ከተቀመጠው የደህንነት ክፍተት ትንተና መስፈርት ጋር በማመሳከር የስጋት ደረጃ ያለው መሆኑን ያረጋግጣል፤

ቀ. በሳይበር ደህንነት ዙሪያ በተቋማት መካከል ቅንጅትና ትብብር እንዲፈጠር እና እንዲጠናከር አስተዋጽኦ ያደርጋል፤

2.3. የሳይበር ደህንነት መሪ (Steering) ኮሚቴ

አጭር መግለጫ

የሳይበር ደህንነት መሪ (Steering) ኮሚቴ ለዘርፉ ቀረቤታ ካላቸው ዳይሬክቶሬቶች /የሥራ ክፍሎች/ በሚወከሉ አካላት ይዋቀራል። መሪ ኮሚቴው በተቋም ውስጥ የሳይበር ደህንነት እሳቤ በግልጽ እና ሁሉን አሳታፊ በሆነ መልኩ እንዲከናወን በተቋሙ ሲታመንበት ይቋቋማል። በመሆኑም ኮሚቴው የሚከተሉት ዋና ዋና ተግባሮች እና ኃላፊነቶች ይኖሩታል። ከዚህ በተጨማሪ አስፈላጊ የሆኑ የመወዳደሪያ አቅሞቹ /Competency/ ከዚህ ሰነድ ጋር አባሪ (ቅጽ 3) ተደርጓል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. የተቋሙን የሳይበር ደህንነት የሥራ ዕቅድ ያዳብራል፣ አፈጻጸም ይከታተላል፤

ለ. የተቋሙ የሥራ ክፍሎች የቴክኖሎጂ ውጤቶች አጠቃቀም በሳይበር ደህንነት እሳቤዎች መሰረት እየተከናወነ መሆኑን ያረጋግጣል፤

ሐ. የሳይበር ደህንነት ስጋት መቀነሻ ስትራቴጂ እንዲቀረጽ የሚመለከተውን አካል ያስተባብራል፣ ስትራቴጂውን ለማስፈጸም የሚያገለግሉ የሳይበር ደህንነት ፕሮጀክቶችንና ተግባራትን በመለየት ምክረ ሃሳብ ያቀርባል፤

መ. የሳይበር ደህንነት ፕሮጀክቶች ትግበራ ላይ ባለድርሻ አካላት እንዲሳተፉ ያስተባብራል፤

ሠ. የሳይበር ደህንነት አስተዳደር /ማኔጅመንት/ ስርዓትን ከሚመለከተው አካል ጋር በመሆን ያዘጋጃል፤

ረ. ታክቲካል የሳይበር ደህንነት የአደጋ/ስጋት/ ዳሰሳ በየስድስት ወሩ ያከናውናል፤ የአደጋ/ስጋት/ ፕሮፋይል ያዘጋጃል፤

ሰ. ለኢንፎርሜሽን ስርዓት ዕውቅና ሰጪ ባለስልጣን የቴክኖሎጂና ስርዓት ደህንነት ፍተሻ መደረጉን በማረጋገጥ የአደጋ/ስጋት/ ደረጃ ተቀባይነት ያለው መሆኑን በመገምገም የኢንፎርሜሽን ስርዓቱ አካል እንዲሆን ይፈቅዳል፣ እውቅና ይሰጣል፤

ሰ. በሳይበር ደህንነት ላይ የሚሰራና ወሳኝ የሆኑ የመረጃ ስርዓቶችን ለሚያስተዳድር ሰራተኛ የይለፍ ፈቃድ (security clearance) መሰጠቱን ያረጋግጣል፤

ሸ. ማንኛውም የሳይበር ጥቃት፣ የፖሊሲና ፕሮሲጀር ጥሰቶችና አጠራጣሪ ሁኔታዎች ሲያጋጥሙ ለሳይበር ደህንነት ዳይሬክቶሬት ያሳውቃል፣ ሪፖርት ያቀርባል፤

2.4. የሳይበር ደህንነት አስተዳደር ቡድን (ክፍል)

አጭር መግለጫ

የሳይበር ደህንነት አስተዳዳር ቡድን (ክፍል) በዋነኝነት የተቋሙን ስጋት አስተዳደር መነሻ በማድረግ የተቋሙን የሳይበር ደህንነት ገዢ ሰነዶች (ፖሊሲዎች፣ ስትራቴጂዎች፣ ስታንዳርዶች፣ መመሪያዎች፣ ሞዴሎች፣ ሜትዶሎጂ፣ ማዕቀፎች) በማበልፀግ በስርዓት እንዲመራ ማድረግ ነው። እንዲሁም የሳይበር ደህንነት ገዢ ሰነዶች ከሃገራዊ የሳይበር ደህንነት ገዢ ሰነዶች ጋር እንዲጣጣም በማድረግ የሳይበር ደህንነትን ለማረጋገጥ በመስኩ ተቋማዊ አቅም መፍጠር ነው። በመሆኑም የቡድኑ (የክፍሉ) ዋና ዋና ተግባር እና ኃላፊነት እንደሚከተለው የተገለጸ ሲሆን የሥራ መደቦች ዝርዝር ደግሞ በዚህ ሰነድ ክፍል ሶስት ተዘርዝረዋል። በተጨማሪም የሥራ ቡድኑ /ክፍሉ/ መሪ ሊኖሩት የሚገቡ የመወዳደሪያ አቅሞች ከዚህ ሰነድ ጋር አባሪ (ቅጽ 4) ተደርጓል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. ተቋማዊ የሳይበር ደህንነት ተልዕኮዎችን ከፖለቲካዊ፣ ከኢኮኖሚያዊ፣ ከማህበራዊ እና ከህጋዊ ፍላጎቶች፣ እንዲሁም ከሥራ ባህል ፍልስፍና፣ ከአለም-አቀፍ ቴክኖሎጂያዊና ከሌሎች አውዳዊ ጉዳዮች አንጻር በመገንዘብና በመተንተን ሥራ ላይ ያውላል፤

ለ. ተቋማዊ ተዕዕኖ ሊፈጥሩ የሚችሉ የሳይበር ደህንነት ፖሊሲዎች፣ ስታንዳርዶች፣ ስትራቴጂዎች፣ መመሪያዎች፣ ሞዴሎች፣ አስተሳሰቦች እና ማዕቀፎች ያበለጽጋል፤

ሐ. የሳይበር ደህንነት ገዢ ሰነዶች በተቋም ውስጥ እንዲተገበሩ ከሚመለከታቸው አካላት ጋር በመቀናጀት ይሰራል፤

መ. የተቋሙን የሳይበር ደህንነት ለመምራት የሚያስችሉ ማዕቀፎችን ያዘጋጃል ይተገብራል፣ ይመራል፣ እንደ አስፈላጊነቱ በየሁለት ዓመቱ ይከልሳል፤

ሠ. በተቀረጹ ተቋማዊ የሳይበር ደህንነት ማኔጅመንት ስርአቶች ላይ የምክክር መድረኮች ያዘጋጃል፣ ይመራል፣ ያቀናጃል፤

ረ. የተቋሙን የሳይበር ደህንነት የስራ ቀጣይነት አስተዳደር ፕሮግራምና እቅድ (Business continuity plan) ይቀርፃል፣ ይዘረጋል፤

ሰ. የአደጋ/የስጋት ማገገሚያ እቅድ እና ፕሮግራም ያዘጋጃል፤ይከታተላል፤

ሸ. በመረጃ፣ በመረጃ ስርዓት እና በመረጃ መሰረተ ልማት ላይ ተግባራዊ የሚደረጉ የሳይበር ደህንነት እሳቤዎች ከሃገሪቱ ህጎችና ደንቦች ጋር የተጣጣሙ እንዲሆኑ ያደርጋል፤

ቀ. የተቋሙን የሳይበር ደህንነት ገዢ ሰነዶች በተመለከተ ለሳይበር ደህንነት ትምህርት/ስልጠና/ ወይም ንቃተ ህሊና ክፍል ስልጠና ፕሮግራም ይቀርፃል፣ የስልጠና ይሰጣል፣ ድጋፍ ያደርጋል፤

2.5. የሳይበር ደህንነት ንቃተ ህሊና ቡድን (ክፍል)

አጭር መግለጫ

የሳይበር ደህንነት ንቃተ-ህሊና ቡድን(ክፍል) በእውቀት፣ በአመለካከት እና በተግባር ማነስ ምክንያት ሊመጣ የሚችለውን የሳይበር ደህንነት ስጋት፣ ተጋላጭነትና ጥቃት በመገንዘብ የሚሰራ ነው። በሳይበር ደህንነት ዋንኛው ተጋላጭ እና በየትኛውም የሳይበር ደህንነት ፕሮግራም ውስጥ የመጀመሪያውና የመጨረሻው የመከላከያ መስመር የሰው ሃይል መሆኑን በመረዳት ለሳይበር ደህንነት ባለሙዎች እና አመራሮች፤ እንዲሁም ለተቋሙ ሰራተኞች የሳይበር ደህንነት ንቃተ ህሊና ፕሮግራሞችን በመቅረጽ፣ በማሰተባበር ይሰጣል። በተጨማሪም በተቋም ውስጥ የሳይበር ደህንነት ባህል እና መሰረታዊ እሳቤዎች እንዲጎለብቱ እና በሰው ሃይል ክፍተት ምክንያት ሊደርስ የሚችለውን የሳይበር ጥቃት እና አደጋ በመቀነስ በመስኩ ተቋማዊ አቅም እንዲፈጠር ማድረግ ነው። በመሆኑም የቡድኑ (የክፍሉ) ዋና ዋና ተግባር እና ኃላፊነት እንደሚከተለው የተገለጸ ሲሆን የሥራ መደቦቹ ዝርዝር ተግባራት ደግሞ በዚህ ሰነድ ክፍል ሶስት ተዘርዝሯል። እንዲሁም የሥራ ቡድኑ(ክፍሉ) መሪ ሊኖሩት የሚገቡ የመወዳደሪያ አቅሞች ከዚህ ሰነድ ጋር አባሪ (ቅጽ 5) ተደርጓል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. የሳይበር ደህንነት ንቃተ-ህሊና ፕሮግራም ይቀርፃል፤ ያዘጋጃል፤ ይመራል፤

ለ. የሳይበር ደህንነት አመራር እና ባለሙያ የሳይበር ደህንነትን ለመምራት የሚያስችል ንቃተ ህሊና እንዳላቸው ቀጣይነት ባለው መንገድ ያረጋግጣል፤

ሐ. የሳይበር ደህንነት ንቃተ-ህሊና ፕሮግራም ስርዓት ንድፍ በማዘጋጀት እና በመተግበር ለአመራሩና ለባለሙያው የሳይበር ደህንነት ዕውቀት ሽግግር ያደርጋል፤

መ. የሳይበር ደህንነት ንቃተ ህሊናና አቅም ግንባታ ስትራቴጂዎች፣ ስልቶች፣ ማዕቀፎች፣ አጀንዳዎች፣ ጽንሰ ሀሳቦች...ወ.ዘ.ተ ያለማል፤

ሠ. የስጋት አስተዳደር ስልጠናዎችን ያዘጋጃል፤ ይመራል፤ ያቀናጃል፤ እንዲሁም በዘርፉ ተቋማዊ አቅም እንዲገነባ ያደርጋል፤

ረ. በሳይበር ደህንነት ፖሊሲዎች፣ ፕሮሲጀሮችና ገዢ ሰነዶች ላይ ስልጠና ይሰጣል፤

ሰ. የሳይበር ደህንነት ንቃተ ህሊና ባህል በተቋም ውስጥ እንዲፈጠር እና እንዲያድግ ያደርጋል፤

ሸ. የተቋሙ ሰራተኞች ያላቸውን የሳይበር ደህንነት ግንዛቤና ንቃተ ህሊና ደረጃ እና የሳይበር ደህንነት ባህልን አስመልክቶ የዳሰሳ ጥናት ያከናውናል፣ ይገመግማል፣ የእርምት እርምጃ ይወስዳል፤

ቀ. የሳይበር ደህንነት ንቃተ ህሊና ሪፖርቶችን ያጠናቅራል፣ ለሚመለከታቸው አካላትም ያቀርባል፤

2.6. የሳይበር ደህንነት ኢንጂነሪንግ ቡድን (ክፍል)

አጭር መግለጫ

የሳይበር ደህንነት ኢንጂነሪንግ ቡድን (ክፍል) በዋነኛነት የተቋሙን ተልዕኮ ለመደገፍ በተዘረጉ የኢንፎርሜሽን ቴክኖሎጂ መሰረተ ልማቶች እና ስርዓቶች ላይ የደህንነት ስጋት እንዳይከሰት የመከላከል፣ የመከታተል፣ የመቆጣጠር እና በየጊዜው አዳዲስ ለውጦችን የማሻሻል ኃላፊነት አለበት። በተቋሙ ፖሊሲ መነሻ የስርዓቶችን ተደራሽነት የሚቆጣጠር እና የሚፈቅድ ይሆናል። እንዲሁም ያልተፈቀዱ ሙከራዎችን ይመረምራል፣ የሳይበር ደህንነት መሳሪያዎችን ያስተዳድራል፣ ለውጥ ያደርጋል፣ ኮንፊገር ያስማማል፣ የደህንነት ክፍተት መዝጊያዎችን (Security patch) እየተከታተለ ያድሳል። በመሆኑም ቡድኑ (ክፍሉ) የሚከተሉት ዋና ዋና ተግባሮች እና ኃላፊነቶች የሚኖሩት ሲሆን የሥራ መደቦቹ ዝርዝር ተግባራት ደግሞ በዚህ ሰነድ ክፍል ሶስት ተዘርዝሯል። በተጨማሪም የሥራ ቡድን /ክፍል/ መሪ ሊኖሩት የሚገቡ የመወዳደሪያ አቅሞች ከዚህ ሰነድ ጋር አባሪ (ቅጽ 6) ተደርጓል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. በተቋሙ ውስጥ ስራ ላይ በሚገኙና በአዳዲስ የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ መሳሪዎች ላይ አስፈላጊውን የደህንነት እርምጃ ይወስዳል፤

ለ. የቴክኖሎጂዎችን ደህንነት በቀጣይነት ሳይቋረጥ እንዲረጋገጥ ያደርጋል፤

ሐ. የሳይበር ደህንነት ኢንጂነሪንግ ፕሮጀክቶች በሃገራዊ የሳይበር ደህንነት ፖሊሲዎች እና ማዕቀፎች መሰረት መሰራታቸውን ያረጋግጣል፤

መ. የተቋሙ የሳይበር ደህንነት ስርዓት ከሃገራዊ የሳይበር ደህንነት ስርዓት ጋር ተናባቢ እንዲሆን ከሚመለከታቸው ባለድርሻ አካላት ጋር በጋራ ይሰራል፤

ሠ. የተለያዩ የሳይበር ደህንነት መፍትሄዎችን ስራ ላይ ያውላል፤ እንዲሁም በተቋሙ ውስጥ ስራ ላይ ለሚገኙ ሁሉም የመረጃ መሰረተ ልማቶች የሳይበር ደህንነት ድጋፍ ይሰጣል፤

ረ. ለተቋሙ በጣም ቁልፍ እና ሚስጥራዊ በሆኑ መረጃዎች ላይ መተግበር ስላለባቸው የሳይበር ደህንነት መሳሪዎች እና ዲዛይኖች ማለትም የጥቃት መከላከል ዘዴዎችን፣ የጥቃት ማስወገድ ዘዴዎችን፣ የመረጃ መጥፋት መከላከያ ዘዴዎችን፣ ፋየርዎል ወ.ዘ.ተ

ላይ የአዋጪነት ጥናት ያደርጋል፤ ለተግባራዊነታቸው ይሰራል፣ ያስተዳድራል፤

ሰ. የተቋሙን የሳይበር ደህንነት ኢንጂነሪንግ ፕሮጀክት ያስተባብራል፤ ያስተዳድራል፤

ሸ. የኢንፎርሜሽን ቴክኖሎጂ መሳሪያዎችን (ሶፍትዌርና ሃርድዌር) የተለያዩ ቴክኖሎጂዎችን በመጠቀም የተቋሙን አውታረ-መረብ ደህንነት ይቆጣጠራል፤

ቀ. ተቋሙ በሚተገብራቸው ቁልፍ የኢንፎርሜሽን ኮምዩኒኬሽን ቴክኖሎጂ ፕሮጀክቶች ላይ የሚመለከታቸው ተቆጣጣሪ አካላት ሙሉ ተሳትፎ እንዲያደርጉና ደህንነታቸውን እንዲያረጋግጡ ምቹ ሁኔታዎችን ያመቻቻል፤

በ. በሳይበር ደህንነት ስጋት ዳሰሳ መነሻ በማንኛውም የመቆጣጠሪያ ስርዓት ላይ አስፈላጊውን የደህንነት ቁጥጥር ስርዓት ይተገብራል፣ ያስተዳድራል፤

ተ. የሳይበር ደህንነትን ሊያዳብር የሚያስችል የቴክኖሎጂ አቅምን ይፈጥራል፤

ቸ. በአደጋ /ስጋት/ ዳሰሳ እና በጥልቀት የመከላከል መርህ መሰረት ወሳኝ የሳይበር ደህንነት ቴክኖሎጂዎችን ስራ ላይ ያውላል፤

ኀ. የኮምፒውተሮችንና የአውታረ-መረቦችን ደህንነት ጠብቆ ይቀምራል (Configure)፣ ይቆጣጠራል፤ ያስተዳድራል፤

ነ. የሳይበር ደህንነት ምርቶችንና አገልግሎቶችን ከሚያቀርቡ /ከሚሰጡ/ አካላት ጋር ያለውን ግንኙነት የተሳለጠ እንዲሆን ምቹ ሁኔታዎችን ይፈጥራል፤ ሂደቱን ይከታተላል፣ የእውቀት ሽግግርና የረጅም ጊዜ እደሳና ጥገና እንዲኖር ያደርጋል፤

ኘ. የሳይበር ደህንነት አስቸኳይ ሁኔታ ሲከሰት እና አደጋ ሲፈጠር የደህንነት ደረጃውን ከፍ ለማድረግ እቅዶችን እና ሂደቶችን ያለማል፤

አ. በተቋሙ ውስጥ የሚገኙ ማናቸውም ሲስተሞች ተደራሽነት የማግኘት ጥያቄዎችን በተቋሙ ፖሊሲ መሰረት ይቆጣጠራል፣ይፈቅዳል፤

ከ. የውስጥ ተጠቃሚዎችን የሲስተም አክሰስ እና ሲስተም ላይ የተሰሩ ስራዎችን ከሎግ በመነሳት ኦዲት ያደርጋል፤

2.7. የሳይበር ደህንነት ኦዲት እና ግምገማ ቡድን (ክፍል)

አጭር መግለጫ

የተቋሙን የሥራ አውድ ባገናዘበ ሁኔታ በሀገር አቀፍና በዓለም አቀፍ ደረጃ የወጡ የሳይበር ደህንነት ስታንዳርዶችን መነሻ በማድረግ የሳይበር ደህንነት ኦዲት እና ምዘና ያከናውናል። በተቋሙ ውስጥ የተተገበሩ ቴክኖሎጂዎችን፣ የተቋሙን የሥራ ሂደት ደህንነት እና የደህንነት ተጋላጭነት በሚመለከት የተቀመጡ መስፈርቶችን፤ እንዲሁም ተቋሙ ሊከተላቸው በወሰናቸው እና በሚገደድባቸው ስታንዳርዶች መነሻ ኦዲት የማድረግ እና የደህንነት ፍተሻ/ምዘና/ በተከታታይነት ማድረግ፣ ለተገኙ ግኝቶችም የመፍትሄ መንገዶችን ይጠቁማል። በተጨማሪ የተቋሙ የሰው ሀይል የተቀመጡ የደህንነት መስፍርቶችን እየተከተለ መሆኑን ይገመግምል፤የደህንነት ንቃተ ህሊና ደርጃቸውን እየመዘነ ክፍተት ባገኘባቸው ቦታዎች የመፍትሄ ምክረ-ሃሳቦችን ያስቀምጣል። በተቋሙ ውስጥ የሚተገበሩ የቴክኖሎጂ ምርቶች ሥራ ላይ ከመዋላቸው በፊት የተቀመጡ የደህንነት መስፈርቶችን ማሟላት ወይም ያለመሟላታቸውን ፍተሻ ያከናውናል። በመሆኑም ዋና ዋና ተግባር እና ኃላፊነት ከታች የተገለጸ ሲሆን፣ የክፍኑ(የቡድኑ) የሥራ መደቦች ደግሞ በዚህ ሰነድ ክፍል ሁለት ተዘርዝሯል። በተያያዘም የሥራ ክፍሉ /ቡድን/ መሪ ሊኖሩት የሚገቡ የመወዳደሪያ አቅሞች /Competency/ ከዚህ ሰነድ ጋር አባሪ (ቅጽ 7) ተደርጓል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. በሀገር እና በአለም አቀፍ ደረጃ የወጡ መመዘኛዎች በመጠቀም ከሰዎች፣ ከቴክኖሎጂና ከሥራ ሂደቶች ጋር ተዛማጅነት ያላቸውን የሳይበር ደህንነት ተጋላጭነቶችን ይለያል፤

ለ. ለሥርዓቱ ደህንነት ሲባል የተቀመጡ የደህንነት መስፈርቶችን ትግበራ ይፈትሻል፤

ሐ. የኢኮቴ ምርቶች ተግባር ላይ ከመዋላቸው በፊት ተቋሙ ያስቀመጣቸውን የደህነነት መስፈርቶች እና የሚከተላቸውን ስታንዳርዶች የሚያሟሉ ስለመሆናቸው ለማረጋገጥ የቅድመ ምዘና ስራ ያከናውናል።

መ. ሀገር አቀፍና አለም አቀፍ ደረጃዎችን መሰረት በማድረግ የተቋሙን ውስጣዊ ተግባሮች ከተቀመጡ ገዢ ሰነዶች አንጻር እየተተገበሩ መሆንና አለመሆናቸውን ኦዲት ያደርጋል፤

ሠ. የተገኙ ክፍተቶችን በደረጃ በማስቀመጥ የመፍትሄ ሃሳቦችን ይጠቁማል፤

ረ. የሳይበር ደህንነት ኦዲት ግኝቶችን ለፕሬዝዳንት /ለዋና ዳሬክተር/ ሥራ አስፈጻሚ ያቀርባል፡፡

2.2. የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ቡድን (ክፍል)

አጭር መግለጫ

ይህ ቡድን (ክፍል) በተቋም ውስጥ የሳይበር ደህንነት ስጋት፣ ተጋላጭነትና ክስተት በፍጥነት እና በአስቸኳይ ለማስወገድ የሚያስችል የመከላከል ሥራ ይሰራል። የተቋሙ የሳይበር ደህንነት ጥቃት የመጀመሪያ ምላሽ ሰጪ አካል ነው። የሥራ ክፍሉ የሳይበር ጥቃቶችን/ችግሮችን/ ዋነኛ መንስኤ በማግኘት ጥቃቱ እንዳይፈጸም እና ዳግመኛ እንዳይከሰት በዋነኛነት ትኩረት አድርጎ የሚሰራ ነው። ይህ ቡድን (ክፍል) የተቋሙን ወሳኝ የመረጃ ስርዓቶች፣ በይነ መረቦች፣ ድሮች እና ሚስጥራዊ ወይም የተከለከለ ውሂብ ጋር የተያያዘ ማንኛውም እውነተኛ ወይም የተጠረጠሩ ክስተቶች የሚከታተል እና ምላሽ የሚሰጥ፤ የተቋሙን የሳይበር ደህንነት ከውስጥ እና ከውጭ ከሚመጣ ክስተትና ጥቃት ይከላከላል። የሥራ ክፍሉ በመስኩ ተቋማዊ አቅም እንዲፈጠር የሚያደርግ፣ መስተጋብር ያለው፣ አውዳዊ፣ ተቋማዊ፣ ሀገራዊ እና አለም አቀፋዊ ሁኔታዎችን ማጤን የግድ የሚለው፣ ስትራቴጂን መሰረት ያደረገ እና ተቋማዊ ተፅዕኖ የሚፈጥር ነው። በመሆኑም ዋና ዋና ተግባሮች እና ኃላፊነቶች ከታች የተገለጹ ሲሆን፣ የክፍሉ (ቡድኑ) የሥራ መደቦች ደግሞ በዚህ ሰነድ ክፍል ሶስት ተዘርዝረዋል። እንዲሁም የሥራ ቡድኑ(ክፍሉ) መሪ ሊኖሩት የሚገቡ የመወዳደሪያ አቅሞች /Competency/ ከዚህ ሰነድ ጋር አባሪ (ቅጽ 8) ተደርጓል።

ዋና ዋና ተግባሮች እና ኃላፊነቶች

ሀ. የሳይበር ደህንነት ተጋላጭነቶችን ያስተዳድራል፤ የተጋላጭነት ክፍተት የመለያ ስትራቴጂዎችን እና አሰራሮችን ያዘጋጃል፣ይተገብራል፤

ለ. የሳይበር ደህንነት ክስተት ቁጥጥር፣ ክትትል እና ምላሽ ስርዓት ይተገብራል፤

ሐ. የተቋሙን የኢንፎርሜሽን ስርዓት ክስተት ደህንነት ይከታተላል፤

መ. የተለያዩ የደህንነት መከላከያ ስርዓቶችን ያቅዳል፣ ይተገብራል፣ያሻሽላል፣ለጥቅም ያውላል፤

ሠ. የሳይበር ደህንነት ክስተት፣ ተጋላጭነትና አደጋ ሪፖርት ያዘጋጃል፤

ረ. በተለያዩ የተቋሙ የስራ ክፍሎች ውስጥ ሊደርሱ የሚችሉ ክስተቶች ወይም የደህንነት ችግር ሊፈጥሩ የሚችሉ አጠራጣሪ ሁኔታዎችን በመለየት ተገቢው የመከላከል እርምጃ እንዲወሰድ ለሚመለከታቸው ክፍሎች ያሳውቃል፤

ሰ. ስርአቶች እና አውታረ-መረቦች በሰርጎ-ገቦች እንዳይጠቁ በንቃት ይቆጣጠራል፤

ሸ. ለሳይበር ደህንነት ችግር የመፍትሄ ለመስጠት የሚያስችል አሰራሮችን ማዘጋጀት፤

ቀ. በሳይበር ደህንነት ጉዳዮች ዙሪያ የትብብር እና የቅንጅት ግንኙነት ይፈጥራል፤

በ. ለሶስተኛ ወገን ክፍት የሚሆኑ ሲስተሞች ላይ ክትትል ያደርጋል፤የተጋላጭነት ሁኔታ ይከታተላል፤

ተ. የሳይበር ደህንነት ጥሰቶችን (security breaches) ዋነኛ ምክንያት ለማወቅ ትንታኔ ይሰራል፤ የተቋሙን ማህበረሰብ ያነቃል (Alert warning) ፤

ቸ. አግባብ የሆኑ የደህንነት መሳሪያዎችን ይጭናል (Installation)፤ የጥንቃቄ እርምጃዎችን አስመልክቶ ምክር ይሰጣል (recommendation) ፤

ኀ. የሳይበር ደህንነት ላይ ያልተለመዱና አጠራጣሪ ሁኔታዎችን በመለየት ችግሮችን ያሳውቃል፤ የአሰራርና ደንብ ጥሰት ሲያጋጥም ለሚመለከተው አካል ያመለክታል፤ ሪፖርት ያደርጋል፤

ነ. የተቋሙን ተጋላጭነት በተገቢ ሁኔታ ያስተዳድራል፤ የተጋላጭነት አያያዝ ስትራቴጂዎችን እና ሂደቶችን ያዘጋጃል፤ ያመቻቻል፤

ኘ. አስፈላጊ የሆኑ የጥበቃ የደህንነት ቴክኖሎጂዎችን የሚመለከቱ ወንጀሎች በወቅቱ ለትክክለኛዎቹ አካላት ሪፖርት ያደርጋል፤

አ. ከተለያዩ የተቋሙ ክፍሎች የሳይበር ጥበቃ ክስተቶችን እና አጠራጣሪ ክስተቶችን ለይቶ ያውቃል፤ ለእነዚህ ክፍሎች የቁጥጥር መመሪያዎችን ያዘጋጃል፤

ከ. የሥራ ክፍሉን ሪፖርት በወቅቱ ለሚመለከተው አካላት ያቀርባል፤

ክፍል ሶስት፡ የሳይበር ደህንነት አደረጃጀት የሥራ መደቦች

የሳይበር ደህንነት አደረጃጀት ወደ ታችኛው እርከን ለማውረድ እና ለመተግበር ያመች ዘንድ ከላይ በክፍል ሁለት የተዘረዘሩትን አደረጃጀቶች ወይም የሥራ ክፍሎች (ቡድኖች) መነሻ በማድረግ ለእያንዳንዱ የሥራ ክፍሎች የሥራ መደብ መጠሪያ እና ደረጃ ተሰጥቷል። እንዲሁም በስምንት(8) ደረጃዎች በመዘርዘር ለእያንዳንዱ የሥራ መደቦች ዋና ዋና ተግባርና ኃላፊነት፣ ዕውቀት፣ ክህሎት፣ የሥራ ልምድ፣ የትምህርት ደረጃ እና ሰርተፍኬሽኖች፤ በተጨማሪ በሥራ መደቦቹ የሚመደቡ ባለሙያዎች ሊኖራቸው የሚገባ የመወዳደሪያ አቅም (Competency) በግልጽ በማስቀመጥ እንደሚከተለው ቀርቧል።

3.1. የሳይበር ደህንነት አስተዳደር ቡድን (ክፍል) የሥራ መደቦች

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: I

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ የተሰጠውን ተልዕኮ በመረዳትና እንደመነሻ በመውሰድ ተግባራትን ያከናውናል፤ ➢ የተሰማራበትን ኢንዱስትሪ ወይም የስራ ዘርፍ በአግባቡ በመረዳት ተግባራትን ያከናውናል፤ ➢ አጠቃላይ የሚሰራበትን ስነ ምህዳር ባህሪያት ይተነትናል፤ ➢ ቡድንን መሰረት ያደረገ የስራ ግንኙነት ይመሰርታል፤ ➢ ሰዎች የሚናገሩትን በአግባቡ ያዳምጣል፤ መልእክቱንም ወደ ራስ ይተረጉማል፤ ➢ የራስን ስራ በተደራጀ መልኩ ያቅዳል፣ ርእታዊ በሆነ የጊዜ ሰሌዳ ውስጥ ስራውን ይሰራል፤ ይከታተላል፤	➢ መሰረታዊ የአሰስመንት እውቀት፤ ➢ መሰረታዊ የኔትወርክ እውቀት፤ ➢ መሰረታዊ ፕሮግራሚንግ እውቀት፤ ➢ መሰረታዊ የሪፖርት አጻጻፍ እውቀት፤ ➢ መሰረታዊ የሴክዩሪቲ እውቀት፤ ➢ የተቋማዊ ተልእኮ እውቀት፤	➢ ከስራው ጋር ተያያዥነት ያላቸው ተቋማዊ ፖሊሲዎችን፣ ስታንዳርዶችን፣ ሂደቶችን፣ ሜትዶሎጆችን እና ቱሎችን የመገንዘብ ክህሎት፤ ➢ ያወቃቸው እውቀቶች ራሱን ለማልማት በአግባቡ የመጠቀም፤ ➢ ክስተቶችን በፍጥነት የመረዳት፤ ➢ የተለያዩ አማራጮች የመገንዘብ፣ የማስተናገድ፤ ➢ ቡድንን መሰረት ያደረገ የስራ ግንኙነት የመመስረት፤ ➢ የሚሰራውን ስራ ስነ-ምህዳር ባህሪያት የመማር፣	የመጀመሪያ ዲግሪ በኮምፒተር ኢንጂነሪንግ፣ በኮምፒተር ሳይንስ፣ በኢንፎርሜሽን ማናጅመንት ሲስተምስ፣ በኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ፡	ከ 0-1 ዓመት	

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ የተለያዩ አማራጮችን መገንዘብ፣ ማስተናገድ፤ እንዲሁም የሌሎች አስተዋፅኦ ጠቃሚ መሆኑ መገንዘብ፤ ➢ ቡድን መሰረት ያደረገ የስራ ግንኙነት መመስረት መቻል፤ ➢ ለሥራ-ዘርፉ የሚሆን እውቀት አጋዥ የሆኑ አካላት መለየት እና አስፈላጊውን እውቀት መጠቀም መቻል፤ ➢ ሰዎች ያሉትን በአግባቡ በማዳመጥ መልእክቱን በአግባቡ ወደ ራስ መተርጎም መቻል፤
➢ የሥራ ክባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች አውዳዊነት ወይም ተጣጣሚነትን ለማረጋገጥ የተቋሙን ራዕይ፣ ተልእኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፖሊቲካዊ፣ ኢኮኖሚካዊ፣ ማህበራዊና ህጋዊ ፍላጎቶች የመረዳት፤ ➢ የስራ ባህል፣ ፍልስፍና፣ ተቋማዊ የስራ-ሂደቶች፣ ሃገራዊና አለም-አቀፋዊ ትስስርን፣ አለም አቀፍ ቴክኖሎጂካዊ አዝማሚያዎች እና ሌሎች አውዳዊ ጉዳዮች የመገንዘብ ብቃት፤
➢ መረጃ የመሰብሰብ ብቃት፤	➢ በቅርበትና በርቀት በሚገኝ የመረጃ ስርዓት ላይ ያሉ ተጋላጭነቶችን ለመለየት የሚረዱ የተለያዩ መረጃዎችን (ምሳሌ ኦፕሬቲንግ ሲስተም፣ ሰርቪስ፣ የተከፈቱ ፖርቶች፣ ወዘተ) የመሰብሰብ ብቃት፤

የሥራ መደብ መጠሪያ፡ የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ፡ II

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ የተሰማራበት ኢንደስትሪ ወይም የስራ ዘርፍ በመገንዘብ ተግባራትን ያከናውናል፤ ➢ የበላይ አካላት /የማናጅመንት/ ይሁንታን ለማግኘት የሚያስችል የግንኙነት እና የተግባቦት አቅም ይገነባል፤ ➢ ጠንካራ የሆነ የቡድን የስራ ግንኙነት ይመሰርታል፤ ➢ በሲስተም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ስጋቶች ይለያል፤ ይተነትናል፤ ➢ ተግባራትን ከጥቅል ተልእኮ ጋር የማስተሳሰር ሥራ በጀማሪ ደረጃ ያከናውናል፤ ➢ የተለያዩ አማራጮችና የሌሎች አስተዋፅኦ ጠቃሚ መሆኑን በመገንዘብ ያስተናግዳል፤ ➢ ለስራ ዘርፉ የሚሆን እውቀት አጋዥ የሆኑ አካላትን በመለየት አስፈላጊውን እውቀት ያሰባስባል፤ ➢ ከሱ ደረጃ በታች ያሉ አባላትን ያሰለጥናል፤ ያበቃል፤	➢ የሳይበር ደህንነት ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ኤጀንት ሞቲቭ (ፍላጎት)፣ የስጋት አይነቶች ግንዛቤ፤ ➢ የሚሰራበት ስነ-ምህዳር እውቀት፤ ➢ የኔትዎርክ ሴክዩሪቲ፤ ➢ የፊዚካል ሴክዩሪቲ፤ ➢ የኢንሲደንት ማናጅመንት፤ ➢ የሪፖርት አጻጻፍ፤ ➢ ሰነድ የመሰነድ፤	➢ የሚሰራበትን ስነ-ምህዳር ባህሪያት የመማር፣ እውቀት የማደራጀትና የማስተሳሰር፤ ➢ በተሰጠው ጉዳይ ላይ ሊያጋጥሙ የሚችሉ የደህንነት ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ኤጀንት ሞቲቭ (ፍላጎት)፣ የስጋት አይነቶች የመለየት፣ የመተንተን እና የማደራጀት፤ ➢ የሚያደርሱ ተፅዕኖዎችን ተቋማዊ የሪስክ አሰስመንት (ስጋት ዳሰሳ) መርሆችና ፍላጎቶች መሰረት በማድረግ የመለየት፣ የመተንተን እና የማደራጀት፤ ➢ ከስራው ጋር ተያያዥነት ያላቸው ተቋማዊ ፖሊሲዎችን፣ ስታንዳርዶችን፣ ሂደቶችን፣ ሜትዶሎጀዎችን እና ቱሎችን ፅንሰ-ሃሳብ የመገንዘብ፤ ➢ ሰዎችን በአግባቡ የማዳመጥ እንዲሁም መልእክቱን በአግባቡ ወደራስ የመተርጎም፤	በኮምፒተር ኢንጂነሪንግ፣ ኮምፒተር ሳይንስ፣ በኢንፎርሜሽን ማናጅመንት ሲስተምስ፣ በኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ፤	ለመጀመሪያ ዲግሪ ከ1-2 ዓመት፤ ለሁለተኛ ዲግሪ ከ0-1 ዓመት አግባብነት ያለው የሥራ ልምድ፤	

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ የተለያዩ አማራጮችን መገንዘብ፣ ማስተናገድ፤ እንዲሁም የሌሎች አስተዋፅኦ ጠቃሚ መሆኑ መገንዘብ፤ ➢ ቡድን መሰረት ያደረገ የስራ ግንኙነት መመስረት መቻል፤ ➢ ለሥራ-ዘርፉ የሚሆን እውቀት አ.ጎ የሆኑ አካላት መለየት እና አስፈላጊውን እውቀት መጠቀም መቻል፤ ➢ በአግባቡ የማዳመጥ እንዲሁም መልእክቱን በአግባቡ ወደ ራስ መተርጎም መቻል፤
➢ የስራ ክባቢ የመገንዘብ ብቃት	➢ የሳይበር ደህንነት አስተዳደር ስራዎች አውዳዊነት ወይም ተጣጣሚነትን ለማረጋገጥ የተቋሙን ራዕይ፣ ተልእኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፖሊቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊና ህጋዊ ፍላጎቶችን መረዳት፣ ➢ የስራ ባህል፣ ፍልስፍና፣ ተቋማዊ የስራ-ሂደቶች፣ ሃገራዊና አለም-አቀፋዊ ትስስርን፣ አለም አቀፍ ቴክኖሎጂያዊ አዝማሚያዎች እና ሌሎች አውዳዊ ጉዳዮች የመገንዘብ ብቃት፤
➢ መረጃ የመሰብሰብ ብቃት	➢ በቅርበትና በርቀት በሚገኙ የመረጃ ስርዓት ላይ ያሉ ተጋላጭነቶችን ለመለየት የሚረዱ የተለያዩ መረጃዎችን (ምሳሌ አፕሬቲንግ ሲስተም፣ ሰርቪስ፣ የተከፈቱ ፖርቶች፣ ወዘተ) የመሰብሰብ ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: III

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ በሲስተም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ተጋላጭነቶችን (risks) ይለያል፣ ይተነትናል፣ ➢ ስርአቶችን (ስታንዳርዶችን፣ ጋይድላይኖችን፣ ሞዴሎች፣ ስትራቴጂዎችን እና ሌሎች ፍሬም ዎርኮችን) ከስተማይዝ ያደርጋል፣ ➢ ከስራው ጋር ተያያዥነት ያላቸው ተቋማዊ ፖሊሲዎችን፣ ስታንዳርዶችን፣ ሂደቶችን፣ ሜትዶሎጂዎችን እና ቱሎችን ፅንሰ-ሃሰብ ሙሉ በሙሉ ይገነዘባል፣ ➢ የደህንነት ክፍተቶችን፣ ስጋቶችን፣ የስጋት ምንጮችን፣ የስጋት ኤጀንት ሞቲቮችን፣ የስጋት አይነቶችን ይተነትናል፣ ይገመግማል፣ ያደራጃል፣ ➢ በተሰጠው ተግባር ላይ ሊያጋጥሙ የሚችሉ/ያጋጠሙ ሪስኮች ወይም ጥቃቶች በጉዳዩ ላይ የሚያደርሱትን ተፅዕኖዎች ይተነትናል፣ ያደራጃል፣ ➢ በሥራ ክፍሎች መካከል ቀጣይና ውጤታማ የሆነ የስራ ግንኙነት ይመሰርታል፣	➢ በሰው ሃይል፣ በስራ ሂደት እና በኢኮቴ መሰረተ-ልማት ላይ የሚኖሩ ክፍተቶች፣ ስጋቶች እና ሪስኮች ዕውቀት፣ ➢ የተቋማዊ ተልዕኮ ዕውቀት፣ ➢ የኢንሲደንት ማናጅመንት ዕውቀት፣ ➢ የአፕሊኬሽን ሴክዩሪቲ ዕውቀት፣ ➢ የኔትዎርክ ሴክዩሪቲ ዕውቀት፣ ➢ የፊዚካል ሴክዩሪቲ ዕውቀት፣ ➢ ተቋማዊ የሳይበር ደህንነት አላማዎች፣ መርሆች፣ ግቦች፣ መዋቅር፣ ራእይ እና ሌሎች አውዳዊ ሁኔታዎች፣	➢ በተሰጠው ጉዳይ ላይ ሊያጋጥሙ የሚችሉ የደህንነት ክፍተቶችን፣ ስጋቶችን፣ የስጋት ምንጮችን፣ የስጋት ኤጀንት ሞቲቭ(ፍላጎት)፣ የስጋት አይነቶችን የመለየት፣ የመገምገም፣ የማደራጀት ➢ የሚያደርሱትን ተጽዕኖዎች ተቋማዊና ሃገራዊ የሪስክ አሰስመንት መርሆችና ፍላጎቶች መሰረት በማድረግ የመለየት፣ የመገምገም፣ የማደራጀት፣ ➢ ለክፍሉ ውጤታማነት አስተዋፅኦ የሚያደርጉ ፍሬምዎርኮችን የማዘጋጀት ክህሎት፣ ➢ ከስራው ጋር ተያያዥነት ያላቸው ተቋማዊ ፖሊሲዎች፣ ስታንዳርዶች፣ ሂደቶች፣ ሜትዶሎጆች እና ቱሎች ፅንሰ-ሃሰብ ሙሉ በሙሉ የመገንዘብ ክህሎት፣ ➢ ሰዎች ያሉትን በአግባቡ የማዳመጥ እንዲሁም መልእክቱን በአግባቡ ወደራስ የመተርጎም ክህሎት፣ ➢ የኢንፎርሜሽን ሴክዩሪቲ ሪስክ	በኮምፒተር ኢንጂነሪንግ፣ በኮምፒተር ሳይንስ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ፣ በኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ፣	ለመጀመሪያ ዲግሪ ከ3-4 ዓመት፣ ለሁለተኛ ዲግሪ ከ1-2 ዓመት አግባብነት ያለው የሥራ ልምድ፣	➢ Comp Security+ (ቢኖር ይመረጣል)

➢ ከደረጃው በታች ያሉ አባላትን ያሰለጥናል፤ ያበቃል፤		መፍትሄ ስታንዳርዶችን መሰረት በማድረግ መምረጥና ማቀናጀት፤ ➢ የተመረጡ መፍትሄዎችንና ፋይዳቸው የማስተሳሰር ክህሎት፤			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ የተለያዩ አማራጮችን መገንዘብ፣ ማስተናገድ፤ እንዲሁም የሌሎች አስተዋፅኦ ጠቃሚ መሆኑ መገንዘብ፤ ➢ ቡድን መሰረት ያደረገ የስራ ግንኙነት መመስረት መቻል፤ ➢ ለሥራ-ዘርፉ የሚሆን እውቀት አጋዥ የሆኑ አካላት መለየት እና አስፈላጊውን እውቀት መጠቀም መቻል፤ ➢ ሰዎች ያሉትን በአግባቡ ማዳመጥ እንዲሁም መልእክቱን በአግባቡ ወደ ራስ መተርጎም መቻል፤
➢ የስራ ከባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች አውዳዊነት ወይም ተጣጣሚነትን ለማረጋገጥ የተቋሙን ራዕይ፣ ተልእኮ፣ ግቦች፣ አላማዎች፣ ፖሊቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊና ህጋዊ ፍላጎቶችን የመረዳት፤ ➢ የስራ ባህል፣ ፍልስፍና፣ ተቋማዊ የስራ-ሂደቶች፣ ሃገራዊና አለም-አቀፋዊ ትስስርን፣ አለም አቀፍ ቴክኖሎጂያዊ አዝማሚያዎች እና ሌሎች አውዳዊ ጉዳዮች የመገንዘብ ብቃት፤
➢ መረጃ የመሰብሰብ ብቃት፤	➢ በቅርበትና በርቀት በሚገኙ የመረጃ ስርዓት ላይ ያሉ ተጋላጭነቶችን ለመለየት የሚረዱ የተለያዩ መረጃዎችን (ምሳሌ ኦፕሬቲንግ ሲስተም፣ ሰርቪስ፣ የተከፈቱ ፖርቶች፣ ወዘተ) የመሰብሰብ ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: IV

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ ከፕሮጀክት በታች የሚታዩ ቡድኖችን ያስተባብራል፤ ለቲሙ ቴክኒካል አስተዋጽኦ ያበረክታል፤ ➢ ከደረጃ IV በታች ያሉ አባላትን ያስለጥናል፤ ያበቃል፤ ➢ በስራ ሂደቱ ላይ የሚኖሩ ባለድርሻ አካላትን ይተነትናል፤ ➢ የበላይ አካላትን ይሁንታ ለማግኘት የሚያስችል የግንኙነት እና የተግባቦት አቅም ይፈጥራል፤ ➢ በሲስተም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ክስተቶች የመለየትና የመተንተን ስርአቶችን (ስታንዳርዶች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ያበለጽጋል፤ ያሻሽላል፤ ➢ ተቋማዊ ፍላጎትን፣ ራእይን፣ አላማን፣ መርሆችን፣ ግቦችን፣ እና	➢ የተቋማዊ ተልእኮ ዕውቀት፤ ➢ የደህንነት ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ኤጀንት ሞቲቮች፣ የስጋት አይነቶች ግንዛቤ፤ ➢ የኢንሲደንት ማናጅመንት ዕውቀት፤ ➢ የአፕሊኬሽን ሴክዩሪቲ፤ ➢ የኔትዎርክ ሴክዩሪቲ፤ ➢ የፊዚካል ሴክዩሪቲ፤ ➢ የሪስክ አሰሳመንት ሜትዶሎጂዎች ወይም ቱሎች፤ ➢ የስጋት ዳሰሳ ጥናትና ትንተና፤ ➢ የሪስክ ማኔጅመንት፤	➢ ተቋማዊ የስራ ሂደቶች ላይ የሚኖሩ ባለድርሻ አካላት የትንተና ክህሎት፤ ➢ ከስራው ጋር ተያያዥነት ያላቸው ተቋማዊ የፖሊሲዎች፣ የስታንዳርዶች፣ የሂደቶች፣ የሜትዶሎጆዎች እና የቱሎች ፅንሰ-ሃሳብ ሙሉ በሙሉ የመገንዘብ ክህሎት፤ ➢ የሚሰራውን ስራ ስነ-ምህዳር ባህሪያት የመማር፣ የማደራጀት እና የማስተሳሰር ክህሎት፤ ➢ ተግባራትን ከጥቅል ተልእኮ ጋር የማስተሳሰር ክህሎት፤ ➢ ቀጣይና ውጤታማ የሆነ ኢንተር-ዲፓርትመንታል የስራ ግንኙነት የመመስረት ክህሎት፤ ➢ የፕሮጀክት አባላትን የማስተባበር፣ ክህሎት፤ ➢ የተለያዩ አማራጮችን የመገንዘብ ክህሎት፤ ➢ ሰዎች የሚናገሩትን በአግባቡ የማዳመጥ እንዲሁም መልእክቱን በአግባቡ ወደራስ የመተርጎም ክህሎት፤ ➢ ውሳኔ የመስጠት ክህሎት፤ ➢ ለክፍሉ ውጤታማነት አስተዋፅኦ የሚያደርጉ ፍሬምዎርኮችን ማዘጋጀት	በኮምፒተር ኢንጂነሪንግ፣ በኮምፒተር ሳይንስ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ፣ በኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ ፡	ለመጀመሪያ ዲግሪ ከ4-5 ዓመት፤ ለሁለተኛ ዲግሪ ከ2-3 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ ISO 27001 lead implementer ወይም ➢ Comp Security+ (ቢኖር ይመረጣል)

ሌሎች አውዳዊ ሁኔታዎችን በጥልቀት ትስስራቸውን በመገንዘብ ይተነትናል፤ ያደራጃል፤ ➢ ወጪ ቆጣቢና ምርጥ የኢንፎርሜሽን ሴኩሪቲ መፍትሄዎችን ይመርጣል፤ ይተነትናል፤ ያደራጃል፤		መቻል፤ ➢ ተቋማዊ የሴክዩሪቲ ፍላጎት፣ አላማ፣ መርሆች፣ ግቦች፣ ራእይ እና ሌሎች አውዳዊ ሁኔታዎችን በጥልቀት መገንዘብ፣ መተንተን፣ ማደራጀት እና ትስስራቸውን የመገንዘብና የማደራጀት ክህሎት፤			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ በሥራ ክፍሎች መካከል ቀጣይና ውጤታማ የሆነ የስራ ግንኙነት መመስረት፤ ➢ ተቋማዊ የሳይበር ደህንነት አስተዳደር ማዕቀፎች ዝግጅት ፕሮጀክቶችን መምራት፤ ➢ የበላይ አካላት/ማኔጅመንት/ ይሁንታ ለማግኘት የሚያስችል የግንኙነት እና የተግባቦት አቅም፤
➢ የድራፍቲንግ/የመሰነድ/ ብቃት፤	➢ በሲስተም ደረጃ እና በተቋም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማኔጅመንት ስርአቶች (ስታንዳርዶች፣ መመሪያዎች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ፅንሰ-ሃሳቦችን እና ፍላጎቶችን ማብላላት፣ ቅጥ ማስያዝ፣ መግለፅ፣ ማያያዝ፣ ማደራጀት እና መሰነድ፤
➢ የመተንተን ብቃት፤	➢ ተቋማዊ የደህንነት ክስተቶች መፍትሄ አቅጣጫ ጭብጥ ሞዴል በቂ ፖለቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊ እና ህጋዊ ፋይዳ ያላቸው መስተጋብር እና ችግር ፈቺነታቸውን ትንተና ማድረግ፤
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ ተቋም ተኮር የሆኑ የሳይበር ደህንነት ፍሬምዎርኮች በተቋሙ ተቀባይነት እንዲያገኙ ማሳመን፣ መግባባት መፍጠር፤ ➢ በተቋም ደረጃ የተዘጋጁ የሳይበር ደህንነት ፍሬምዎርኮች ምን ያክል ፋይዳ እንዳላቸው ፍንትው አድርጎ ማሳየት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: V

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ ተቋማዊ የሴክዩሪቲ ፍላጎት፣ ራእይ፣ አላማ፣መርሆች፣ግቦች፣መዋቅር፣ እና ሌሎች አውዳዊ ሁኔታዎችን በጥልቀት ይተነትናል፣ ያደራጃል፣ ያስተሳስራል፤ ➢ በሲስተም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማናጅመንት ስርአቶች (ስታንዳርዶች፣ ጋይድላይኖች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ያበለጽጋል፤ ያሻሽላል፤ ➢ ተቋማዊ የስራ ሂደቶች ላይ የሚኖሩ ባለድርሻ አካላት ተግባር ይተነትናል፤ ➢ ተቋማዊ ግንኙነት ወይም ትስስር መፍጠር የሚያስችሉ ሂደቶችን ይቀርጻል፤ ➢ የሳይበር ደህንነት ከተቋማዊ ተልዕኮ፣ ፍላጎት፣ ፍልስፍና፣ እሴት እና የስራ ባህል ያላቸውን ትስስር ይተነትናል፤ ➢ ማዕቀፎች ፣ ሞዴሎች እና አርክቴክቸሮችን ይነድፋል፤ ➢ ለማናጀሮች እና ለስራ አስፈፃሚዎች ሰፊ ስትራተጂክ ምክር ይሰጣል፤ ➢ ፕሮጀክት ይመራል፤	➢ ተቋማዊ የሴክዩሪቲ ፍላጎት፣ራዕይ፣ አላማ፣ መርሆች፣ ግቦች፣ መዋቅር እና ሌሎች አውዳዊ ሁኔታዎች፤ ➢ የደህንነት ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ኤጀንት ሞቲቮች፣ የስጋት አይነቶች የላቀ እውቀት፤ ➢ አካላዊ/ቁሳዊ/፣ ከባቢያዊ፣ ቴክኒካዊ፣ ሂደቶች እና ሰውን መሰረት ያደረጉ የሳይበር ደህንነት መቆጣጠሪያዎች ዕውቀት፤ ➢ ኢንተርናሽናል የሳይበር ደህንነት ስታንዳርዶች፣ ሞዴሎች፣ አርክተክቸሮች፣ ሜትዶሎጂዎች እና ሌሎች ፍሬምዎርኮች፤ ➢ ኢንፍራስትራክቸር ሴክዩሪቲ ዕውቀት፤	➢ ተቋማዊ የሴክዩሪቲ ፍላጎትን፣ ራዕይ፣ አላማ፣ መርሆች፣ግቦች፣መዋቅር እና ሌሎች አውዳዊ ሁኔታዎችን በጥልቀት መገንዘብ፣ መተንተን፣ ማደራጀት እና ትስስራቸውን የመገንዘብና የማደራጀት ክህሎት፤ ➢ የስራ ሂደቶች ትስስርን በአግባቡ የመለየት፣ የመገንዘብ፣ የመተንተንና የማደራጀት ክህሎት፤ ➢ የባለድርሻ አካላት ትንተና ማድረግ፤ ➢ ወጪ ቆጣቢና ምርጥ የኢንፎርሜሽን ሴኩሪቲ የመፍትሄ አቅጣጫዎችን የመምረጥ፣ የመገምገምና የማቀናጀት ክህሎት፤ ➢ ተቋማዊ ቅንጅት ወይም ትስስር የመፍጠር ክህሎት፤ ➢ ተልዕኮ መሰረት ያደረገ የግንኙነት ክህሎት፤	በኮምፒተር ኢንጂነሪንግ፣ ፣ በኮምፒተር ሳይንስ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ፣ በኢንፎርሜሽን ቴክኖሎጂ እና በተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ ፡	ለመጀመሪያ ዲግሪ ከ5-6 ዓመት፣ ለሁለተኛ ዲግሪ ከ3-4 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ CEH ወይም ➢ ISO 27001 lead implementer ወይም ➢ project management ወይም ➢ risk management (ቢኖር ይመረጣል)

➢ የስራ ሂደት ይቀርጻል፤ ይተገብራል፤ ➢ ከደረጃው በታች ያሉ አባላትን ያሰለጥናል፤ ያበቃል፤ ➢ የተለያዩ የስራ ሂደቶችን ትስስር/ተመጋጋቢነት/ በአግባቡ ይለያል፣ ይገነዘባል፣ ይተነትናል፤ ያደራጃል፤ ➢ ፈጠራና ግኝት በተሞላበት አኳሃን መፍትሄዎች ያመጣል፤ ➢ ተግባራዊ የተደረጉ የሳይበር ደህንነት መቆጣጠሪያዎችን ውጤታማነት ይተነትናል፤ ➢ ቁልፍ እና ከፍተኛ ደረጃ ካላቸው ባላድርሻ አካላት ጋር አብሮ ይሰራል፤		➢ የተመረጡ መፍትሄዎችና ፋይዳቸውን የማስተሳሰር ክህሎት፤ ➢ በስራ ዘርፎች የተለዩ ፅንሰ-ሃሳቦችን እና የሴክዩሪቲ ፍላጎቶችን ማብላላት፣ ቅጥ የማስያዝ፣ የማስተሳሰር፣ የማደራጀ እና የመሰነድ ክህሎት፤ ➢ ተቋማዊ ቁልፍ ጉዳዮች እና ሀብቶች ላይ ሊያጋጥሙ የሚችሉ የደህንነት ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ኤጀንት ሞቲቮች፣ የስጋት አይነቶች የሪሰክ አሰስመንት መርሆችንና ፍላጎቶችን መሰረት በማድረግ የመለየት፣ የመገምገም፣ የማደራጀት፤ ➢ በተቋማዊ ተልዕኮ ቁልፍ ጉዳዮች እና ሀብቶች ላይ ያጋጠሙ/ ሊያጋጥሙ/ የሚችሉትን የሴክዩሪቲ ክስተቶች ተቋሙ እና ከተቋሙ ጋር ግንኙነት ያላቸው አካላት ላይ የሚያደርሱትን ተፅእኖ			

		የመተንተን፣ የመገምገም፣ የማደራጀት፤			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ ድራፍቲንግ/ የመሰነድ/ ብቃት፤	➢ በተቋም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማኔጅመንት ስርአቶች (ስታንዳርዶች፣ ጋይድላይኖች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ፅንሰ-ሃሳቦችን እና ፍላጎቶችን ማብላላት፣ቅጥ ማስያዝ፣ መግለፅ፣ ማያያዝ፣ ማደራጀት እና መሰነድ፤
➢ የመተንተን ብቃት፤	➢ ተቋማዊ የሴክዩሪቲ ክስተቶች መፍትሄ አቅጣጫ ጭብጥ ሞዴል በቂ ፖለቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊ እና ህጋዊ ፋይዳ ያላቸው መስተጋብር እና ችግር ፈቺነታቸውን ትንተና ማድረግ፤
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ በሥራ ክፍሎች መካከል ቀጣይና ውጤታማ የሆነ የስራ ግንኙነት መመስረት፤ ➢ ተቋማዊ የሳይበር ደህንነት አስተዳደር ማዕቀፎች ዝግጅት ፕሮጀክቶችን መምራት፤ ➢ የበላይ አካላት/ማኔጅመንት/ ይሁንታ ለማግኘት የሚያስችል የግንኙነት እና የተግባቦት አቅም፤
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ ተቋም ተኮር የሆኑ የሳይበር ደህንነት ፍሬምዎርኮች በተቋሙ ተቀባይነት እንዲያገኙ ማሳመን፣ መግባባት መፍጠር፤ ➢ በተቋም ደረጃ የተዘጋጁ የሳይበር ደህንነት ፍሬምዎርኮች ምን ያክል ፋይዳ እንዳላቸው ፍንትው አድርጎ ማሳየት፤
➢ የመፍጠርና የማሻሻል ብቃት፤	➢ በሲስተም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማኔጅመንት ስርአቶች (ስታንዳርዶች፣ መመሪያዎች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ማበልፀግ፣ ማሻሻል፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: VI

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ በተቋም ደረጃ ተፅእኖ ያላቸው የሳይበር ደህንነት ማኔጅመንት መርሆች፣ ሞዴሎች፣ ሜትዶሎጂዎች፣ የስራ ሂደቶች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች ይቀምራል፣ ያበለጽጋል፤ እንዲሁም ለተቀባይነታቸውና ተግባራዊነታቸው ተፅእኖ ይፈጥራል፤ ➢ ሃገራዊ ፖለቲካዊ ፣ ኢኮኖሚያዊ፣ ማህበራዊ፣ ህጋዊ ፍላጎቶች፣ መርሆች፣ ፍልስፍናዎች እና ሌሎች አውዳዊ ሁኔታዎችን በጥልቀት ይገነዘባል፣ ይተነትናል፣ ያደራጃል፣ ያስተሳስራል፤ ➢ የስራ አከባቢው ባለድርሻ አካላትን ይለያል፤ ይተነትናል፤ ተጣጣሚነትን ያረጋግጣል፤ ➢ በመስኩ ሃገራዊ ቅንጅት እንዲመጣ ይሰራል፤ ➢ ፈጠራና ግኝት በተሞላበት አካኋን መፍትሄዎችን ያመጣል፤ ➢ ከአንድ በላይ ፕሮጀክቶችን ይመራል፤	➢ የሳይበር ደህንነት ገቨርናንስ ፅውቀት፤ ➢ የተቋማዊ ባህልና ባህሪ (የስራ-ሂደት፣ ስራ-ሂደት ዘርፍ፣ መዋቅር፣ የስራ ባህል፣ አስተሳሰብ፣ ተልእኮ፣ ራዕይ፣ግብ፣ አላማ ወዘተ) ፅውቀት፤ ➢ የፕሮግራም፣ የፕሮጀክት የማናጅመንት ፅውቀት፤ ➢ የቢዝነስ ስትራተጂ ፅንሰ ሃሰቦች እውቀት፤ ➢ የባለ ድርሻ አካላት እና የሶስተኛ ወገን ማኔጅመንት ፅውቀት፤	➢ ሃገራዊ ፖለቲካዊ ፣ ኢኮኖሚያዊ፣ ማህበራዊ፣ ህጋዊ ፍላጎቶች፣ መርሆች፣ ፍልስፍናዎች እና ሌሎች አውዳዊ ሁኔታዎችን በጥልቀት የመገንዘብ፣ የመተንተን፣ የማደራጀት እና የማስተሳሰር ክህሎት፤ ➢ ባለድርሻ አካላትን የመለየት እና የመተንተን ክህሎት፤ ➢ መፍትሄ ከችግሮች ፈልቅቆ የማውጣት ክህሎት፤ ➢ የማሳመን ክህሎት፤ ➢ በዘርፎች የተለዩ ፅንሰ-ሃሳቦችን እና የሴኩሪቲ ፍላጎቶችን የማብላላት፣ ቅጥ የማስያዝ፣ የማስተሳሰር፣ የማደራጀት እና የመሰነድ ክህሎት፤ ➢ ተቋማዊ ቁልፍ መሰረተ-ልማቶች ላይ የሚደረገውን የኢንፎርሜሽን ሪስክ አሰስመንት ፕሮግራም የማቀድ፣የመምራት፣ የመገምገም ክህሎት፤ ➢ በተቋማዊ ተልዕኮና ወሳኝ ሀብቶች ላይ የሚደረገውን የኢንፎርሜሽን ሪስክ ትንተና ፕሮግራም የማቀድ፣ የመምራት፣ የመገምገም፤	በኮምፒተር ኢንጂነሪንግ፣፣ በኮምፒተር ሳይንስ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ፣ በኢንፎርሜሽን ቴክኖሎጂ እና በተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ ፡	ለመጀመሪያ ዲግሪ ከ6-7 ዓመት፣ ለሁለተኛ ዲግሪ ከ4-5 ዓመት አግባብነት ያለው የሥራ ልምድ፣	➢ CEH ወይም ➢ CRISK ወይም ➢ ISO 27001 lead impleme nter ወይም ➢ Project manage ment ወይም ➢ Risk manage ment (ቢኖር ይመረጣል)

➢ ማዕቀፎች ፣ ሞዴሎች እና አርክቴክቸሮች ይነድፋል፤ ➢ ከደረጃው በታች ያሉ አባላትን ያሰለጥናል፤ ያበቃል፤ ➢ ሁሉን አቀፍ ተቋማዊ የደህንነት ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ኤጀንት ሞቲቮች፣ የስጋት አይነቶች ይለያል፣ ይገመግማል፤ ያደራጃል፤ ➢ ተቋማዊ ሪስክ ማናጅመንት ፕሮግራም ያቅዳል፣ ይመራል፣ ይቀምራል፤ ➢ ተቋማዊ የሳይበር ደህንነት ሪስክ ሚቲጌሽን(የስጋት ማለዘቢያ) ስትራቴጂ ይነድፋል፤ ➢ ሃገራዊ የሳይበር ደህንነት ሪስኮች ለይቶ ያወጣል፤ ➢ በተሰማራበት ዘርፍ ስትራቴጂክ እቅድ ይቀርጻል፤ ይተገብራል፤ ➢ ተቋማዊ የሳይበር ደህንነት ማናጅመንት ስራዎችን ይለካል፣ ይገመግማል፣ ተግባራዊነታቸውን ይከታተላል፤		➢ ሃገራዊ ሪስክ ትንተና መሰረት በማድረግ ወጥና ምክኒያታዊ የሆነ ሁሉ አቀፍ የሪስክ መፍትሄ ስትራተጂ የመንደፍ ክህሎት፤ ➢ የፅንሰ-ሀሳቦች ፋይዳ፣ መስተጋብር፣ ችግር ፈቺነታቸው ትንተና የማድረግ ክህሎት፤ ➢ መሳኢ አዝማሚያዎች በጥልቀት የመገንዘብ፣ የመተንተን እና ወደራስ የማስተሳሰር ክህሎት፤ ➢ አብሮ የመስራት ክህሎት፤ ➢ ችግሮችን የመለየት ክህሎት፤ ➢ ችግሮችና የመፍትሄ አቅጣጫዎችን የማስተሳሰር፣ ፋይዳቸውን የማስላት ክህሎት፣ ➢ ፍላጎቶችን የማብላላት፣ ቅጥ የማስያዝ፣ የማስተሳሰር፣ የማደራጀት እና የመሰነድ ክህሎት፤			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ ድራፍቲንግ/ የመሰነድ/ ብቃት፤	➢ በሲስተም ደረጃ እና በተቋም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማኔጅመንት ስርአቶች (ስታንዳርዶች፣መመሪያዎች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ፅንሰ-ሃሳቦችን እና ፍላጎቶችን ማብላላት፣ቅጥ ማስያዝ፣ መግለፅ፣ ማያያዝ፣ ማደራጀት እና መሰነድ፣
➢ የሙተንተን ብቃት፤	➢ ተቋማዊ የሴክዩሪቲ ክስተቶች መፍትሄ አቅጣጫ ጭብጥ ሞዴል በቂ ፖለቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊ እና ህጋዊ ፋይዳ፣ ያላቸው መስተጋብር እና ችግር ፈቺነት ትንተና ማድረግ፣
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ በሥራ ክፍሎች መካከል ቀጣይና ውጤታማ የሆነ የስራ ግንኙነት መመስረት፣ ➢ ተቋማዊ የሳይበር ደህንነት አስተዳደር ማዕቀፎች ዝግጅት ፕሮጀክቶችን መምራት፣ ➢ የበላይ አካላት/ማኔጅመንት/ ይሁንታ ለማግኘት የሚያስችል የግንኙነት እና የተግባቦት አቅም፣
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ ተቋም ተኮር የሆኑ የሳይበር ደህንነት ማዕቀፎች በተቋሙ ተቀባይነት እንዲያገኙ ማሳመን፣ መግባባት መፍጠር፤ ➢ በተቋም ደረጃ የተዘጋጁ የሳይበር ደህንነት ፍሬምዎርኮች ምን ያክል ፋይዳ እንዳላቸው ፍንትው አድርጎ ማሳየት፤
➢ የመፍጠርና የማሻሻል ብቃት፤	➢ በሲስተም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማኔጅመንት ስርአቶች (ስታንዳርዶች፣ጋይድላይኖች፣ ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ማበልፀግ፣ ማሻሻል፤
➢ ችግሮችንና መፍትሄዎችን የማስተሳሰር ብቃት፤	➢ በሲስተም ደረጃ የሚለዩት የሪስኮች የመፍትሄ አቅጣጫዎች የተቋሙን ፍላጎት፣ ነባራዊ ሁኔታን የሚመልሱና ሁሉ አቀፍ መሆናቸውን ማረጋገጥ፤ ➢ የተለዩ የመፍትሄ አቅጣጫዎች የሚያስገኙትን ትክክለኛ ጥቅም ማስላት፤ ➢ የተለዩ የመፍትሄ አቅጣጫዎች የጎንዮሽ ጉዳት እንዳይኖራቸው ማረጋገጥ፤ ➢ እያንዳንዱን ሪስክ መፍትሄ እንደተቀመጠላት ማረጋገጥ፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: VII

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ በሴክተር ደረጃ ተፅእኖ ያላቸው የሳይበር ደህንነት ማኔጅመንት መርሆችን፣ ሞዴሎችን፣ ሜትዶሎጂዎችን፣ የስራ ሂደቶችን፣ ስትራቴጂዎችንና ሌሎች ማዕቀፎችን ይቀምራል፣ ያበለጽጋል፣ ተቀባይነታቸውን ይከታተላል፤ ➢ ሃገራዊ የኢንፎርሜሽን ደህንነት ማናጅመንት ማዕቀፎች ብልፀጋ ፕሮጀክቶች ላይ ይሳተፋል፤ ➢ ሃገራዊ የሳይበር ደህንነት ሪስኮች የመፍትሄ አቅጣጫ ስትራቴጂን ለይቶ ያወጣል፤ ➢ የሳይበር ደህንነት ፍላጎቶች ተጣጣሚነትን ያረጋግጣል፤ ➢ የተሰማራበትን ዘርፍ ስትራቴጂክ እቅድ ይቀርጻል ፣ ይተገብራል፤ ➢ የሃገራዊ ፍላጎቶችንና የተሰማራበትን ምህዳር ጥልቅ አረዳድና አዝማሚያዎች ያነባል፣ ይተነትናል፣ የአዝማሚያዎቹን ተጽእኖ	➢ የቢዝነስ ስትራቴጂ ፅንሰ- ሃሰቦች፤ ➢ የተቋማዊ አውዳዊ ኩነቶች ፖሊቲካዊ፣ ማህበራዊ፣ ኢኮኖሚያዊ እና ህጋዊ ሁኔታዎች፤ ➢ የስትራቴጂ፣ የፖሊሲ ንድፍ፤ ➢ ተቋማዊ የሳይበር ደህንነት ስታንዳርዶች፣ ሜትዶሎጂዎች፣ ሞዴሎች፣ መመሪያዎች፣ ምርጥ ተሞክሮዎች እና ፍሬምዎርኮች፤ ➢ የስርአት ንድፈ-ሃሳብ፤ ➢ የሳይበር አስተዳደር፤ ➢ የቅንጅታዊ-ስርአት፤ ➢ የፕሮጀክት ማኔጅመንት እውቀት፤	➢ የሳይበር ደህንነት ፍሬምዎርክ ኮንሰፕት(ጭብጥ) ሞዴል የመቅረፅ/ የማዘጋጀት ክህሎት፤ ➢ መፃኢ አዝማሚያዎችን በጥልቀት የመገንዘብ፣ የመተንተን እና ወደ ራስ የማስተሳሰር ክህሎት፤ ➢ አብሮ የመስራት ክህሎት፤ ➢ ክፍለ አህጉራዊና አለም አቀፋዊ ቅንጅትን የመፍጠር ክህሎት፤ ➢ ችግሮችና የመፍትሄ አቅጣጫዎች የማስተሳሰር፣ ፋይዳቸውን የማስላት ክህሎት፤ ➢ የማሳመንና የመደራደር ክህሎት፤ ➢ ፅንሰ-ሃሳቦችንና ፍላጎቶችን የማብላላት፣ ቅጥ የማስያዝ፣ የማስተሳሰር፣ የማደራጀት እና የመሰነድ ክህሎት፤ ➢ በሃገራዊ ወሳኝ ጉዳዮች እና ሀብቶች ላይ ያጋጠሙ/ ሊያጋጥሙ የሚችሉትን የሴክዩሪቲ ክስተቶች በተቋም ወይም በሃገር ደረጃ የሚያደርሱትን ተፅእኖ የመተንተን፣ የመገምገም፣ የማደራጀት ክህሎት፤ ➢ ሃገራዊ ወይም ዓለም አቀፋዊ ተፅእኖ ሊፈጥሩ የሚችሉ የሪስክ አሰስመንትና	በኮምፒተር ኢንጂነሪንግ፣ ፣ በኮምፒተር ሳይንስ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ፣ በኢንፎርሜሽን ቴክኖሎጂ እና በተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ ፡	ለመጀመሪያ ዲግሪ ከ7-8 ዓመት፤ ለሁለተኛ ዲግሪ ከ5-6 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ CISM ወይም ➢ CISSP ወይም ➢ CISO ወይም ➢ CEH ወይም ➢ CRISK ወይም ➢ ISO 27001 lead implementer ወይም ➢ ITIL ወይም ➢ Project management ወይም ➢ Risk management (ቢኖር ይመረጣል)

ይተነብያል፤ ➢ ከደረጃው በታች ያሉ አባላትን ያሰለጥናል፣ ያበቃል፤ ➢ የሳይበር ደህንነት ሪስክ ማገገሚያ ስትራቴጂ ውጤት ይለካል፤ ➢ ሃገራዊ የኢንፎርሜሽን ደህንነት ሪስክ ማናጅመንት ፕሮጀክቶችን ይመራል፤ ➢ ሃገራዊ የሳይበር ደህንነት ሪስኮችን ለይቶ ያወጣል፤ ➢ ተቋማዊ፣ ሃገራዊ እና አለም አቀፋዊ እይታዎችን ይተነትናል፤		ትንተና መርሆች፣ ሞዴሎች፣ ሜትዶች፣ ሂደቶች እና ሌሎች አዳዲስ ንድፈ-ሃሳቦችን የመቀመር፣ የማበልፀግ፤ ➢ ወጥና ምክንያታዊ የሆነ ሁሉን አቀፍ የሪስክ ትንተና ስትራቴጂ የመንደፍ፤ ➢ ሀሳቦችን የማያያዝ፣ የማደራጀት እና ቅጥ እንዲይዝ የማድረግ ክህሎት፤ ➢ መፃኢ አዝማሚያዎችን በጥልቀት የመገንዘብ፣ የመተንተን እና ወደ ራስ የማስተሳሰር ክህሎት፤			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የማስተባበርና የማቀናጀት ብቃት፤	➢ ተግባራት በሚገባ ሁኔታ እንዲከናወኑ አስፈላጊ ቁሳቁሶችን የማሟላት፣ የጊዜ ሰሌዳውን የመቅረፅ፣ ለሚመለከታቸው አካላት የማሳወቅ እና ስራው በተሳካ ሁኔታ እንዲሰራ ቀድሞ መሰራት ያለባቸውን ስራዎች በሚገባ የማስተባበርና የማቀናጀት ብቃት፣
➢ የመፍጠርና የማሻሻል ብቃት፤	➢ በተቋም ደረጃ ተግባራዊ የሚደረጉ የሳይበር ደህንነት ማኔጅመንት ስርአቶችን (ጋይድላይኖች፣ሞዴሎች፣ ስትራቴጂዎች እና ሌሎች ፍሬምዎርኮች) ማበልፀግ እና ማሻሻል፤
➢ ችግሮችንና መፍትሄዎችን የማስተሳሰር ብቃት፤	➢ በተቋም ደረጃ የሚለዩት ሪስኮችና የመፍትሄ አቅጣጫዎች የተቋሙን ፍላጎት እና ነባራዊ ሁኔታን የሚመልሱ መሆናቸውን ማረጋገጥ፤ ➢ በተቋም ደረጃ የሚለዩት ሪስኮች፣ የሚቀመጡት የመፍትሄ አቅጣጫዎች ሁሉን አቀፍ መሆናቸውን ማረጋገጥ፤ ➢ የተለዩ የመፍትሄ አቅጣጫዎች የሚያስገኙትን ትክክለኛ ጥቅም ማስላት፤ ➢ የተለዩ መፍትሄዎች የጎንዮሽ ጉዳት እንዳይኖራቸው ማረጋገጥ፤ ➢ እያንዳንዷን ሪስክ የመፍትሄ አቅጣጫ እንደተቀመጠላት ማረጋገጥ፤
➢ የማማከር ብቃት፤	➢ የተቋሙን ከፍተኛ አመራሮች በሳይበር ደህንነት ዙሪያ ማማከር፤
➢ ጉዳዮችን በተለያዩ አቅጣጫዎች የማየት ብቃት፤	➢ የሳይበር ደህንነት ስርዓት ቀረጻ እና ትግበራ ላይ ከተለያየ አቅጣጫዎች (ከፖለቲካ፣ ከማህበራዊ፣ ከኢኮኖሚ፣ ከህጋዊ፣ ወዘተ..) የማየትና ሁለንተናዊነትን በተላበሰ አኳሃን የመቃኘት፣ የመገንዘብ በኮምፒተንሲው ዙሪያም የማማከር ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አስተዳደር ባለሙያ

ደረጃ: VIII

ዋና ዋና ተግባርና ኃላፊነት	እውቀት	ክህሎት	የትምህርት ደረጃ	የሥራ ልምድ	ሰርተፍኬት
➢ በዘርፉ አለም-አቀፍ ፖለቲካዊ፣ ማህበራዊ፣ ኢኮኖሚያዊ እና ህጋዊ ሁኔዎችን ይተነብያል፣ ይተነትናል፤ ➢ የሳይበር ደህንነት የመፍትሄ አቅጣጫ ስትራቴጂ ኮንሰፕት ሞዴል ይቀርጻል፤ ➢ ሃገራዊ ወይም አለም አቀፍ ተፅእኖ ሊፈጥሩ የሚችሉ የሳይበር ደህንነት ማኔጅመንት መርሆችን፣ ሞዴሎችን፣ ስታንዳርዶችን፣ ፖሊሲዎችን፣ ሜትዶሎጂዎችን፣ ስትራቴጆዎችን፣ የአሰራር-ሂደቶችን እና ሌሎች አዳዲስ ንድፈ-ሀሳቦችን ይቀምራል፣ ያበለጽጋል፤ ተቀባይነታቸውንና ተግባራዊነታቸውን ይከታተላል፤ ➢ የሳይበር ደህንነት ማኔጅመንት ሃገራዊና አለም-አቀፋዊ ተጣጣሚነትን ያረጋግጣል፤	➢ የሃገራዊ አውዳዊ ኩነቶች ፖለቲካዊ፣ ማህበራዊ፣ ኢኮኖሚያዊ እና ህጋዊ ሁኔታዎች፤ ➢ አለም-አቀፋዊ ሁኔታዎች (ከሳይበር ደህንነት ጋር ተያይዞ) ግንዛቤ፤ ➢ ፖሊሲና ስትራቴጂ የመንደፍ፤ ➢ አለም-አቀፋዊ ወይም ሃገራዊ የሳይበር ደህንነት ስታንዳርዶች፣ ሜትዶሎጂዎች፣ ሞዴሎች፣ መመሪያዎች፣ ምርጥ ተሞክሮዎች እና ሌሎች ፍሬምዎርኮች ዕውቀት፤ ➢ የውጤታማነት ቅንጅት ዕውቀት፤	➢ ወጥና ምክንያታዊ የሆነ ሁሉን አቀፍ የሳይበር ደህንነት የመፍትሄ አቅጣጫ ስትራቴጂ ኮንሰፕት ሞዴል የመቅረፅ ፤ ➢ ሃገራዊ ወይም አለም አቀፋዊ ተፅእኖ ሊፈጥሩ የሚችሉ የሳይበር ደህንነት ማኔጅመንት መርሆች፣ ሞዴሎች፣ ስታንዳርዶች፣ ፖሊሲዎች፣ ሜትዶሎጂዎች፣ ስትራቴጂዎች፣ የአሰራር-ሂደቶች፣ ጋይድላይኖች እና ሌሎች አዳዲስ ንድፈ-ሀሳቦችን የመቀመር፣ የማበልፀግ፤ ➢ ሁሉን አቀፍ የሪስክ መፍትሄ ስትራቴጂ ተፈፃሚነትን መለካት እንዲሁም ለተፈፃሚነቱ ተፅእኖ የመፍጠር ብቃት፤ ➢ በሃገራዊ ቁልፍ መሰረተ-ልማት ላይ የሚደረገውን የሳይበር ደህንነት ሪስክ ትንተና ፕሮግራም የማቀድ፣ የመምራት፣ የማቀናጀት፣	በኮምፒተር ኢንጂነሪንግ ወይም በኮምፒተር ሳይንስ ወይም በማናጅመንት ኢንፎርሜሽን ሲስተምስ ወይም በኢንፎርሜሽን ቴክኖሎጂ እና በተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ወይም የሁለተኛ ዲግሪ፤	ለመጀመሪያ ዲግሪ ከ8-9 ዓመት፣ ለሁለተኛ ዲግሪ ከ6-7 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ CISM ወይም ➢ CISSP ወይም ➢ CISO ወይም ➢ CEH ወይም ➢ CRISK ወይም ➢ ISO 27001 lead implementer ወይም ➢ ITIL ወይም ➢ Project management ወይም ➢ Risk management (ቢኖር ይመረጣል)

		የመገምገም ብቃት፤ ➢ አጠቃላይ ሃገራዊ የሳይበር ደህንነት ማናጅመንት ጉዳዮች ላይ መንግስትን የማማከር ክህሎት፤ ➢ መሳኢ አዝማሚያዎችን በጥልቀት የመገንዘብ፣ የመተንተን እና ወደ ራስ የማስተሳሰር ክህሎት፤			
➢ ሃገራዊ የሳይበር ደህንነት ማኔጅመንት ጉዳዮች ላይ መንግስትን በማማከር ሂደት ድርሻ ያበረክታል፤ ➢ ጥናታዊ ፅሑፎችን ያዘጋጃል፤ ➢ በመስኩ አለም- አቀፋዊ ግንኙነትን ይፈጥራል፤ ➢ ተቋማዊ፣ አገራዊ እና አለም አቀፋዊ እይታዎችን ይቀርጻል፤ ➢ ሃገራዊ የኢንፎርሜሽን ደህንነት ሪስክ ማናጅመንት ፕሮጀክቶችን ይመራል፤ ➢ ሃገራዊ የሳይበር ደህንነት ሪስኮች እንድምታቸውን ይተነትናል፤ ➢ የሃገራዊ ፍላጎቶችንና የተሰማራበትን ምህዳር ጥልቅ አረዳድ እና አዝማሚያዎች ያነባል፣ ይተነትናል፣ የአዝማሚያዎቹን ተጽእኖ ይተነብያል፤					

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የማስተባበርና የማቀናበር ብቃት፤	➢ ተግባራት በሚገባ ሁኔታ እንዲከናወኑ አስፈላጊ ቁሳቁሶችን የማሟላት፣ የጊዜ ሰሌዳውን የመቅረፅ፣ ለሚመለከታቸው አካላት የማሳወቅ እና ስራው በተሳካ ሁኔታ እንዲሰራ ቀድሞ መሰራት ያለባቸውን ተግባራት በሚገባ የማስተባበርና የማቀናበር ብቃት፣
➢ ችግሮችንና መፍትሄዎች የማስተሳሰር ብቃት፤	➢ በተቋም ደረጃ የሚለዩት ሪስኮች፣ የመፍትሄ አቅጣጫዎች፣ የተቋሙን ፍላጎትና ነባራዊ ሁኔታን የሚመልሱ መሆናቸውን ማረጋገጥ፤ ➢ በተቋም ደረጃ የሚለዩ ሪስኮች፣ የሚቀመጡት የመፍትሄ አቅጣጫዎች ሁሉን አቀፍ መሆናቸውን ማረጋገጥ፤ ➢ የተለዩ የመፍትሄ አቅጣጫዎች የሚያስገኙትን ትክክለኛ ጥቅም ማስላት፤ ➢ የተለዩ መፍትሄዎች የጎንዮሽ ጉዳት እንዳይኖራቸው ማረጋገጥ፤ ➢ እያንዳንዷን ሪስክ የመፍትሄ አቅጣጫ እንደተቀመጠላት ማረጋገጥ፤
➢ የማማከር ብቃት፤	➢ የተቋሙ ከፍተኛ አመራሮችን በሳይበር ደህንነት ጉዳይ ማማከር፤
➢ በተለያየ አቅጣጫ የማየት ብቃት፤	➢ የሳይበር ደህንነት ስርዓት ቀረጻ እና ትግበራ ላይ ከተለያዩ አቅጣጫዎች (ከፖለቲካ፣ከኢኮኖሚ፣ማህበራዊ፣ ወዘተ..) በማየት ሁለንተናዊነትን በተላበሰ አኳሃን የመቃኘት፣ የመገንዘብ በኮምፒተንሲው ዙሪያም የማማከር ብቃት፤

3.2. የሳይበር ደህንነት ንቃተ ህሊና ቡድን (ክፍል) የሥራ መደቦች

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ: I

ዋና ዋና ተግባር እና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች /ስልጠናዎች/
➢ ለንቃተ ህሊና ስልጠና ፕሮግራሞች የሚያስፈልጉ መረጃዎችን ያሰባስባል፤ ➢ የስልጠና እና ንቃተ ህሊና ፕሮግራም ስርዓት ንድፍ ለማዘጋጀት የሚያስችል የዳሰሳ ጥናት መረጃዎችን ያሰበስባል፤ ➢ አለማቀፋዊ፣ ቀጠናዊና ሃገራዊ የሳይበር ደህንነት ክስተቶች ላይ ወቅታዊ መረጃዎችን ይሰበስባል፤ ➢ የንቃተ-ህሊና ማጎልበቻና ባህል መገንቢያ ፕሮግራሞችን ለመፈተሽ የሚያስችሉ መረጃዎችን ይሰበስባል፤ ➢ ተቋማዊ የደህንነት አጠባበቅ መመሪያዎችን ይከታተላል፤ ያብራራል፤ ➢ ለተቋማዊ የንቃተ-ህሊናና ባህል ግንባታ ምዘና የሚያገለግሉ መረጃዎችን ይሰበስባል፤	➢ የለሙ የንቃተ ህሊና እና ተቋማዊ ባህል ዳሰሳ ስርዓቶች ዕውቀት፤ ➢ የተለዩ የዳሰሳ መንገዶች እና ሰውን መመዘኛና የማብቂያ መንገዶች ዕውቀት፤ ➢ የተለዩ የትምህርት፣ ስልጠና፣ ንቃተ-ህሊናና የባህል ግንባታ አመራር ስርዓቶች ዕውቀት፤ ➢ የተለያዩ የንቃተ-ህሊናና ባህል ግንባታ ማዕቀፎችና ስርዓቶች ግንዛቤ፤ ➢ የተነደፉ የንቃተ-ህሊናና ባህል ግንባታ ስልት/ስትራቴጂዎች/ ግንዛቤ፤	➢ መሰረታዊ የተግባቦት ክህሎት፣ የማዳመጥ እና ግብረ-መልስ የመቀበል ክህሎት፤ ➢ በሰው ምክንያት ሊመጡ የሚችሉ የደህንነት ስጋቶች ቀድሞ የመረዳት ክህሎት፤ ➢ የተተነተኑ ሰውን የማበልጸጊያ መንገዶችን የመረዳት ክህሎት፤ ➢ ደህንነት ከሰው ጋር ያለውን መስተጋብር በመተንተን የመለየት ክህሎት፤	በኮምፒተር ሳይንስ፣ በኮምፒተር ኢንጂነሪንግ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ፣በኢንፎርሜሽን ቴክኖሎጂ እና በተዛማጅ የሙያ ዘርፍ፤ ወይም በሳይኮሎጂ፣ በሶሺዮሎጂ እና በተዛማጅ የሙያ ዘርፍ የመጀመሪያ ዲግሪ፤	0-1	

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ በቡድን የመስራት ብቃት፤	➢ የተቋሙን ተልዕኮ ለመደገፍ፤ ግቦችን ለማሳካትና ለማጠናከር የሳይበር ደህንነት ንቃተ ህሊና ፕሮግራም መገንዘብ፤
➢ ጥልቅ የንባብ ክህሎት፤	➢ ጥልቀት ያለዉ ዘርፈ ብዙ የንቃተ ህሊናና ባህል ማሳልበቻ ፅንሰ ሃሳቦችን፣ ማዕቀፎችን፣ ልምዶችንና ጥናቶችን አንብቦ በአውዳዊነት የመረዳት አቅም፤
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ ከስራ ባልደረቦቹና ከተቋሙ ሰራተኞች ጋር ተባብሮ መረጃዎችን የመሰብሰብ አቅም፤
➢ የመረጃ መተንተንና መተርጎም ብቃት፤	➢ አለም አቀፍ፣ አህጉር አቀፍና ሃገራዊ የሳይበር ደህንነት ክስተቶችን ተከታትሎ መረጃዎችን ተንትኖ የማቅረብ ብቃት፤

የሥራ መደብ መጠሪያ፡ የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ
ደረጃ፡ II

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ስርተፍኬቶች
➢ ለሳይበር ደህንነት ንቃተ ህሊና ስልጠና ፕሮግራሞች የሚያስፈልጉ መረጃዎችን ያሰባስባል፤ ➢ የሳይበር ደህንነት ትምህርት፣ ስልጠና እና ንቃተ-ህሊና ፕሮግራም ስርዓት ንድፍ ለማዘጋጀት የሚያስችል የዳሰሳ ሥራ መረጃዎችን ያሰባስባል፤ ➢ በሳይበር ደህንነት ፖሊሲ እና ፕሮሲጀር ገዢ ሰነዶች ላይ ስልጠና ለመስጠት የሚያስችሉ መረጃዎችን ያሰባስባል፣ ➢ የሳይበር ደህንነት ንቃተ ህሊናና ስልጠና ፕሮግራም ለማዘጋጀት የሚረዱ ግብዓቶችን ያሰባስባል፤ ➢ ሰራተኞች በተሰጣቸው የይለፍ (የፈቃድ) ደረጃ መጠን መብትና የተከለከሉትን ጉዳዮች መለየትና የይለፍ (የፈቃድ) ደረጃ እና ክልከላ ከመደረጉ በፊት ማብራሪያ ይሰጣል፤ ➢ የተቋሙ ሰራተኞች ያላቸውን የሳይበር ደህንነት ንቃተ ህሊና ደረጃ ለመገምገምና በውጤቱም መሰረት አስፈላጊውን የእርምት እርምጃ ለመውሰድ የሚያስችሉ መረጃዎችን ያሰባስባል፤	➢ የለሙ የሳይበር ደህንነት ንቃተ ህሊና የዳሰሳ ስርዓቶች ዕውቀት፤ ➢ የተለዩ የዳሰሳ መንገዶች እና ሰውን መመዘኛና የማብቂያ መንገዶች ዕውቀት፤ ➢ የተለዩ የሳይበር ደህንነት የትምህርት፣ ስልጠናና ንቃተ ህሊና አመራር ስርዓቶች ዕውቀት፤ ➢ የሳይበር ደህንነት ንቃተ ህሊና ማዕቀፎችና ስርዓቶች ግንዛቤ፤ ➢ የተነደፉ የሳይበር ደህንነት ንቃተ ህሊና ስልት/ስትራቴጂዎች ግንዛቤ፤ ➢ የሳይበር ደህንነት ንቃተ-ህሊና በተቋም ውስጥ የመፍጠር እና የማሳደግ ግንዛቤ፤	➢ መሰረታዊ የተግባቦት ክህሎት፣ የማዳመጥ እና ግብረ-መልስ የመቀበል ክህሎት፤ ➢ በሰው ምክንያት ሊመጡ የሚችሉ የሳይበር ደህንነት ስጋቶች ቀድሞ የመረዳት ክህሎት፤ ➢ የተተነተኑ ሰውን የማበልጸጊያ መንገዶችን የመረዳት ክህሎት፤	በኮምፒተር ሳይንስ፣ በኮምፒተር ኢንጂነሪንግ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ፤ በኢንፎርሜሽን ቴክኖሎጂ እና በተዛማጅ የሙያ ዘርፍ ወይም ሳይኮሎጂ፣ ሶሺዮሎጂ እና ተመሳሳይ የሙያ ዘርፍ የመጀመሪያ ዲግሪ ወይም ሁለተኛ ዲግሪ	ለመጀመሪያ ዲግሪ ከ1-2 ዓመት፤ ለሁለተኛ ዲግሪ ከ0-1 ዓመት፤	

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ በቡድን የመስራት ብቃት፤	➢ የተቋሙን ተልዕኮ ለመደገፍ፤ ግቦችን ለማሳካት እና ለማጠናከር የሳይበር ደህንነት ንቃተ ህሊና ፕሮግራም መገንዘብ፤ ➢ የተቋሙን አውድ ከግንዛቤ ውስጥ በማስገባት የሳይበር ደህንነት ባህል በተቋም ውስጥ በተጨባጭ ለመፍጠር ከተቋሙ ማህበረሰብ ጋር በቅርበት በቡድን የመስራት ብቃት፤
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ የተለያየ የሥራ ባህል እና የስራ ከባቢ፣ ማህበራዊ እምነት፣የትምህርት ድህረ-ታሪክ፣ የሙያ ድህረ-ታሪክ ያላቸው እና በተለያዩ እድሜ ክልል የሚገኙ ሰዎችን በሙያዊ ስነ-ምግባር፣ በጥንቃቄ፣ ውጤታማነትን በሚያጎናፅፍ መልኩ እና መልካም ስነ-ምግባር በተላበሰ አኳሃን ተግባብቶ አብሮ ለመስራት የሚያስችል ብቃት፤
➢ የግንኙነት ብቃት፤	➢ የሳይበር ደህንነት ሁኔታን በተመለከተ መረጃውን ሊያውቁ ለሚገባቸው አካላት እንዲተላለፍ የማድረግ ብቃት፤ ➢ የሳይበር ደህንነት ከሚመለከታቸው አካላት ጋር በሚኖሩ ውይይቶች እና ሌሎች ግንኙነቶች እራስን የመግለጽ ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ: III

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራልምድ	ሰርተፍኬቶች
➢ በተቋም ደረጃ አጀንዳና ይዘቶች/ዝርዝር/ ማኑዋሎችን ያለማል፣ ➢ አጀንዳዎች ተደራሽ የሚደረጉበት የግንኙነት ዘዴ ይወስናል፣ ➢ በተቋም ደረጃ ባህሪ/ባህል/ የፍላጎት ዳሰሳ ያከናውናል፣ ➢ ተቋማዊ ስልጠናዎችን ይሰጣል፤ ➢ የስልጠና መንገዶችን ይለያል፤ ➢ የግምገማ ዳታዎችን ይተነትናል፤ ሰንዶ ያስቀምጣል፡ ➢ ተቋማዊ የስልጠና ፍላጎት ዳሰሳዎችን ያከናውናል፣	➢ የተሰጠውን ችግር መሰረት በማድረግ የባህሪ/ባህል/ ዳሰሳ ለማከናወን የሚያስችል ግንዛቤ፤ ➢ የከባቢ ግንዛቤ፣ ለምሳሌ፡- ተቋማዊ ጉዳዮች፣ ተቋማዊ የአሰራር ስርዓቶች፣ ባህል፣ የግለሰብ ባህሪ፣ሃገራዊ ጉዳዮች(ሃገራዊ አጀንዳዎች)፣ የልማት እንቅስቃሴዎች፣ ባለድርሻ አካላት (አጥቂ፣ ተጠቂ)፤ ➢ የለውጥ/ግንባታ/ ግቦችን ግንዛቤ፤ ➢ የለውጥና የለውጥ አስተዳድር ግንዛቤ፤ ➢ የኢላማዎች (ተቋም፣ ግለሰብ፣ ቡድኖች፣ ወ.ዘ.ተ.) ግንዛቤ፤ ➢ የባህሪ/ባህል ለውጥ አላማና ግቦች ግንዛቤ፤ ➢ የባህሪ/ባህል ችግሮችን የመረዳት ብቃት፤ ➢ በተቋም ደረጃ ያሉ ባህሪ/ባህል ችግሮችን የመረዳት ብቃት፣	➢ ጥሬ ዳታ/ኢንፎርሜሽን/ ምንጭ በተለዩ ስርዓታዊ በሆኑ መንገዶች ግንኙነት፣ ምክንያትና ውጤትን፣ ክፍተትን የማወቅ፣ የመገምገም እና ዶክመንት የማድረግ፤ ➢ በደረጃው ምክረ ሃሳቦችን የመሰነድ፤ ➢ ከባቢ የመገንዘብና የመረዳት፤ ➢ የባህሪ/ባህል ለውጥ/ግንባታ ስልጠናዎች የመስጠት፤ ➢ የኮሙኒኬሽን ቻነል የመለየት የመምረጥ፤ ➢ የተነደፉ የባህሪና የባህል ግንባታ/ለውጥ መንገዶች/ እና ዒላማዎች የመለየት፣ በቅደም ተከተል (Priority) የማስቀመጥ ብቃት፤ ➢ አነስተኛ መጠን ያላቸው መፍትሄዎችን ዲዛይን የማድረግ ክህሎት፤ ➢ የራስ ስራን የማቀድ፣	በኮምፒተር ሳይንስ፤ በኮምፒተር ኢንጂነሪንግ፣ በማናጅመንት በኢንፎርሜሽን ሲስተምስ ወይም በኢንፎርሜሽን ቴክኖሎጂ እና በተዛማጅ የሙያ ዘርፍ፤ ወይም ሳይኮሎጂ፣ ሶሺዮሎጂ እና በተዛማጅ የሙያ ዘርፍ የመጀመሪያ ወይም ሁለተኛ ዲግሪ፤	➢ ለመጀመሪያ ዲግሪ ከ2-4 ዓመት የስራ ልምድ፤ ➢ ለሁለተኛ ዲግሪ 0-2 ዓመት በተንዳኝ የስራ መስክ የሰራ/ች፤	

			➢ ለራስ ስራ ዝርዝር ግቦችንና መለኪያዎችን የማውጣት፤ ➢ በደረጃው ስርአታዊ በሆነ መንገድ ሪፖርት የማድረግ፤ ➢ መልዕክት/ኢንፎርሜሽን/ ታዳሚን በሚመጥን ደረጃ በፅሁፍ/በገለፃ/ የማቅረብ ብቃት፤ ➢ መለስተኛ የኮምፒውተር ክህሎቶች፤ ➢ ከስራ አጋሮች ጋር ውጤታማ ግንኙነት የመፍጠር ክህሎት፤		

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የግጭት አስተዳደር ብቃት (Conflict management)፤	➢ የሚለሙ ስትራቴጂዎች፣ ሞዴሎች፣ ሜተዶሎጂዎች፣ ፕሮግራሞች፣ ማዕቀፎች እና ካሪኩለሞች ጋር የሚኖረውን መስተጋብር የመገንዘብና መፍትሄዎችን ዲዛይን የማድረግ ብቃት፣
➢ የማስተሳሰር (Alignment) ብቃት፤	➢ የተለዩ አጀንዳዎችና ኮንሰፕቶች ከኢላማዎች እንቅስቃሴ ጋር የማቆራኘት እና ትስስር የመፍጠር ብቃት፤
➢ ችግር የመፍታት ብቃት፤	➢ ችግሮችን የመለየትና የመተንተን፣ የኢንፎርሜሽን ትክክለኛነትና ጠቀሜታ የመመዘን፣ መፍትሄ የሚሆኑ አማራጮች የማፍለቅ እና የመገምገም፣ ምክረ-ኃሳብ የማመንጨት ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ: IV

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራልምድ	ሰርተፍኬቶች
➢ በተቋም ደረጃ የፍላጎት ዳሰሳዎችን ያዘጋጃል፣ ይመራል፤ ➢ የአጀንዳ/የኮንሰፕት/ መልዕክት ይዘት እንዲሁም ተደራሽ የማድረጊያ መንገድ ውጤታማነት ይገመግማል፤ ➢ የስልጠና መንገዶችን ዲዛይን ያደርጋል፤ ➢ ተቋማዊ ስልጠናዎችን ይመራል፤ ➢ ተቋማዊ የለውጥ ግምገማዎችን ይመራል፤	➢ የሚላማ ቀረጻ ዕውቀት፤ ➢ የኮሙኒኬሽን ፅንስ ሃሳብ የመተንተን (ዲዛይን) የማድረግ ዕውቀት፤ ➢ ላኪ-መልእክት ቻነል ተቀባይ (ግብረ-መልስ)፤ ➢ የተለዩ የግምገማ ስርዓቶች፣ስልቶችና መመዘኛዎች ዕውቀት፤ ➢ በተቋም ደረጃ ያሉ የባህሪ/ባህል/ ችግሮች ግንዛቤ፤ ➢ በተቋም ደረጃ ያሉ የባህሪ/ባህል ለውጥ/ ግንባታ ችግሮችን የመለየት፣ የመረዳትና የመተንተን፤	➢ የባህሪ/ባህል/ ለውጥ ኮንሰፕት የማልማት ብቃት፤ ➢ የባህሪ/ባህል ለውጥ የስልጠና ማንዋል የማልማት ብቃት፤ ➢ ተቋማዊ ትስስር የመፍጠር ክህሎት፤ ➢ ተቋማዊ ተፅእኖ የመፍጠር ክህሎት፤ ➢ በተቋም ደረጃ ተግባራዊ የሚሆኑ የባህሪ/ባህል ለውጥ/ግንባታ/ መንገዶችን ተግባራዊ ማድረግ፤ ➢ የባለድርሻ አካላት ፍላጎት የመረዳት ብቃት፣ የባለድርሻ አካላት ትንተና የማካሄድ ብቃት (ተሳታፊ ባለድርሻ አካላት)፤ ➢ ውጤታማ ተፅእኖ የመፍጠሪያ መንገዶች/ቻነሎች/ የመንደፍ፤ ➢ የተለየ ሚላማን የመገምገም ክህሎት፤ ➢ በተለዩ የግምገማ ስርአቶች መሰረት ከባቢ/ሚላማ/ ለውጥ የመገንዘብ፤ ➢ በየደረጃው ትምህርት የሚወሰድባቸውን ጉዳዮች ቀምሮ የመሰነድ፤	የመጀመሪያ ወይም ሁለተኛ ዲግሪ በኮምፒተር ሳይንስ፤ በኮምፒተር ኢንጂነሪንግ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ወይም ኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ፤ ወይም ሳይኮሎጂ፣ ሶሺዮሎጂ እና ተመሳሳይ የሙያ ዘርፍ፤	➢ የመጀመሪያ ዲግሪ 4-6 ዓመት የስራ ልምድ፤ ➢ ሁለተኛ ዲግሪ 2-4 ዓመት የሥራ ልምድ	➢ CSAP (Certified Security Awareness Practitioner) (ቢኖር ይመረጣል)

		➢ በተቋም ደረጃ አጀንዳዎችን፣ ጭብጦችና ይዘቶችን ከኢላማዎች ጋር የማስተሳሰር፣ ➢ መፍትሄዎችንና አማራጮችን የማመንጨትና ዲዛይን የማድረግ፣ ➢ በተቋም ውስጥ የሚገኙ የተለያዩ ባህሎችን እና ግለሰባዊ ልዩነቶችን የመቀበል፣የማስተናገድ፤ ➢ በክፍል ደረጃ ካሉ አባላት ጋር ውጤታማ ግንኙነት የመመስረት ብቃት፣ ➢ ለሌሎች የቡድን አባላት ተገቢ የሆነ ድጋፍ የመስጠት ብቃት፣			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ (Description)
➢ የግጭት አስተዳደር ብቃት (Conflict management)፤	➢ የሚለሙ ስትራቴጂዎች፣ ሞዴሎች፣ ፕሮግራሞች፣ ማዕቀፎችና ካሪኩለሞች የሚኖራቸውን መስተጋብር የመገንዘብና መፍትሄዎችን ዲዛይን የማድረግ ብቃት፣
➢ የማስተሳሰር ብቃት፣	➢ የተለዩ አጀንዳዎችን፣ ኮንሰፕቶችን ከኢላማዎች ጋር የማቆራኘት እና ትስስር የመፍጠር ብቃት፣
➢ ችግር መፍታት፤	➢ ችግሮችን የመለየትና የመተንተን፣ የኢንፎርሜሽን ትክክለኛነትና ጠቀሜታ የመመዘን፣ መፍትሄ የሚሆኑ አማራጮች የማፍለቅ እና የመገምገም፣ ምክረ-ኃሳብ የማመንጨት ብቃት፤
➢ ዕቅድና ቅንጅት፤	➢ ፍላጎቶችን በመለየት ዝርዝር ግቦችን ከዳር ማድረስ የሚያስችል ራስን ወይም ሌሎችን የሚያካትት ዝርዝር ተግባራትን የመቅረፅ እና የተግባራቱ አፈፃፀም ግቦቹን ለማሳካትና ለመከታተል የሚያስችል መመዘኛ ስርዓት የማበጀት ብቃት፤
➢ ተግባቦት፤	➢ ኢንፎርሜሽን እና ኃሳብ በብቃትና ግልፅ በሆነ በቃል እና/ወይም በፅሁፍ የማቅረብና የመግለፅ፤ ➢ ሌሎች የሚናገሩትን የማዳመጥ እና የመረዳት፤ ➢ ኢንፎርሜሽንንና ኃሳብን ለሌሎች የማጋራት ወይም ከሌሎች ጋር የመለዋወጥ፤ ➢ ሙሉ እና ጊዜውን የጠበቀ ወይም ታዳሚን ያገናዘበ ውሳኔ የመስጠት እና ሌሎች ሊስማሙበት በሚችሉበት መንገድ ኢንፎርሜሽንና ማቴሪያሎች የማቅረብ ብቃት፤
➢ ከሰዎች ጋር ግንኙነት የመፍጠር ብቃት፣	➢ የሌሎችን ስሜት፣ ፍላጎት እና አቅም የመገንዘብ እና ተገቢ ምላሽ የመስጠት፤ ➢ ምቹና ምቹ ባልሆነ ሁኔታ የሰዎችን ደረጃ፣ የስራ ሁኔታ፣ ወዘተ እንደ መመዘኛ ባለማስቀመጥ በብቃት ስራን የመስራት፣ የባህል እና ኢንተርፐርሰናል ልዩነቶችን የመቀበል፤ ➢ ግጭቶችና አለመስማማቶች ሲያጋጥሙ የተሳታፊዎቹ ስሜት እና ምላሽ መቆጣጠር በሚያስችል መንገድና በማለሰቦቹ የሚደርስ አሉታዊ ተፅእኖ በሚቀንስ አዎንታዊ በሆነ መንገድ የመፍታት እና ተገቢ የሆነ ድጋፍ የመስጠት ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ: V

ዋና ዋና ተግባር እና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራልምድ	ሰርተፍኬቶች /ስልጠና/
➢ ፕሮጀክት ይመራል፤ ➢ የባህል ግንባታና ባህሪ ለውጥ ስትራቴጂዎች፣ ሞዴሎች፣ ፕሮግራሞች፣ ማዕቀፎች እና ካሪኩለሞች ለማልማት አስፈላጊውን ተቋማዊ ቅኝት (Observation) ያከናውናል፤ ➢ ተቋማዊ ፍላጎትን መነሻ ያደረጉ የባህሪ ለውጥና የባህል ግንባታ ስትራቴጂዎች፣ ሞዴሎች፣ ካሪኩለሞች፣ ፕሮግራሞች እና ማዕቀፎችን ያለማል፤ ➢ በተቋም ደረጃ ተፅዕኖ የሚፈጥሩ የባህሪ/ባህል/ አጀንዳዎችን ይለያል፤ ይመርጣል እና ዲዛይን ያደርጋል፤ ➢ የተዘጋጁ አጀንዳ/ኮንሰፕት/ኮንተንት እንዲሁም ተደራሽ የማድረጊያና ውጤታማነት የመገምገሚያ መስፈርቶች በማውጣት ይገመግማል፤ ➢ የባህሪ/ባህል/ ንቃተ ህሊናና ስልጠና መንገዶችን ዲዛይን ያደርጋል፤	➢ የባህሪ/ባህል የዳሰሳ ዒላማ የመለየት፤ ➢ የባህሪ/ባህል ችግር የመለየት፤ ➢ የዳሰሳ የትኩረት ከባቢ/ዒላማ የመለየት ብቃት፤ ➢ የዳሰሳ መንገዶች የመለየት ብቃት፤ ➢ በቡድን ደረጃ ክንውኖችና ዝርዝር ተግባራት ዕቅድ ማውጣት፣	➢ በተቋም ደረጃ የባህሪ/ባህል/ ዳሰሳ የማከናወን፤ ➢ በዳሰሳው ተግባራዊ የሚሆኑ መመዘኛዎች የመለየት፤ ➢ በተቋማት ደረጃ ተፅእኖ መፍጠር የሚችል ዳሰሳ ጥናት ዲዛይን የማድረግና የመምራት፤ ➢ በተቋማት ደረጃ ተፅእኖ መፍጠር የሚችሉ የዳሰሳ ሪፖርቶች፤ ➢ በተቋም ደረጃ በዳሰሳ ዙሪያ የማማከር፤ ➢ ምክረ-ኃሳብ ቀምሮ የመሰነድ፤ ➢ በደረጃው ምክረ ኃሳቦችን የመሰነድ ብቃት፤ ➢ በተቋም ደረጃ የተፈጠረውን ተፅእኖ (Impact) የመገምገም፤ ➢ የግምገማ ስርዓት የመለየት፤ ➢ የግምገማ መስፈሪያዎችን የማውጣት፤	የመጀመሪያ ወይም ሁለተኛ ዲግሪ በኮምፒተር ሳይንስ፤ በኮምፒተር ኢንጂነሪንግ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ወይም ኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ፤ ወይም በሳይኮሎጂ፣ ሶሺዮሎጂ እና ተመሳሳይ የሙያ ዘርፍ፤	➢ የመጀመሪያ ዲግሪ 6-8 ዓመት የስራ ልምድ፤ ➢ ሁለተኛ ዲግሪ 4-6 ዓመት የሥራ ልምድ	➢ MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program ወይም ➢ CSAP (Certified Security Awareness Practitioner) ወይም ➢ PMP – Project Management Professional (ቢኖር ይመረጣል)

➢ የንቃተ ህሊና ፕሮግራሞችን በመቅረጽ ተቋማዊ ትስስር ይፈጥራል፤		➢ የመገምገምና ለውጥ (እድገት/ክፍተት) የመለየት፤ ➢ የአፈፃፀም መገምገምያ መስፈርቶች የማውጣት፤ ➢ በደረጃው የተወሰዱ ትምህርቶችን ሰንዶ ማስቀመጥ፤ ➢ በመካከለኛ መጠን የስራ ክንውኖችን፣ ተግባራትንና ሪፖርቶችን ስርአታዊ በሆነ መንገድ በፅሁፍና በንግግር የመግለፅ፤ ➢ በደረጃው የሚለሙ አጀንዳዎች፣ ጭብጦችና ይዘቶች ታዳሚዎችን በሚመጥን ሁኔታ የማቅረብ፤ ➢ ከባለ ድርሻ አካላት ጋር ውጤታማ ግንኙነት የመመስረት፤ ➢ በደረጃው ስርአታዊ በሆነ መንገድ የስራ ክንውኖችን ሪፖርት የማድረግ፤ ➢ ኢላማን በመካከለኛ መጠን የመገንዘብ፤ ➢ በሃገር ደረጃ ብዝሃነትን መቀበል፤			

ከባለድርሻ አካላት (ተቋማት፣ ግለሰቦች ወ.ዘ.ተ.) ጋር ውጤታማ ግንኙነት መፍጠር።					

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የግጭት አስተዳደር ብቃት (Conflict management)፤	➢ የሚለሙ ስትራቴጂዎች፣ ሞዴሎች፣ ፕሮግራሞች፣ ማዕቀፎችና ካሪኩለሞች የሚኖራቸውን መስተጋብር የመገንዘብና መፍትሄዎችን ዲዛይን የማድረግ ብቃት፣
➢ የማስተሳሰር ብቃት፤	➢ የተለዩ አጀንዳዎችን፣ ኮንሰፕቶችን ከኢላማዎች ጋር የማቆራኘት እና ትስስር የመፍጠር ብቃት፣
➢ ችግር መፍታት፤	➢ ችግሮችን የመለየትና የመተንተን፣ የኢንፎርሜሽን ትክክለኛነትና ጠቀሜታ የመመዘን፣ መፍትሄ የሚሆኑ አማራጮች የማፍለቅ እና የመገምገም፣ ምክረ-ኃሳብ የማመንጨት ብቃት፤
➢ ዕቅድና ቅንጅት፤	➢ ፍላጎቶችን በመለየት ዝርዝር ግቦችን ከዳር ማድረስ የሚያስችል ራስን ወይም ሌሎችን የሚያካትት ዝርዝር ተግባራትን የመቅረፅ እና የተግባራቱ አፈፃፀም ግቦቹን ለማሳካትና ለመከታተል የሚያስችል መመዘኛ ስርዓት የማበጀት ብቃት፤
➢ ተግባቦት፤	➢ ኢንፎርሜሽን እና ኃሳብ በብቃትና ግልፅ በሆነ በቃል እና/ወይም በፅሁፍ የማቅረብና የመግለፅ፤ ➢ ሌሎች የሚናገሩትን የማዳመጥ እና የመረዳት፤ ➢ ኢንፎርሜሽንንና ኃሳብን ለሌሎች የማጋራት ወይም ከሌሎች ጋር የመለዋወጥ፤ ➢ ሙሉ እና ጊዜውን የጠበቀ ወይም ታዳሚን ያገናዘበ ውሳኔ የመስጠት እና ሌሎች ሊስማሙበት በሚችሉበት መንገድ ኢንፎርሜሽንና ማቴሪያሎች የማቅረብ ብቃት፤
➢ ከሰዎች ጋር ግንኙነት የመፍጠር ብቃት፤	➢ የሌሎችን ስሜት፣ ፍላጎት እና አቅም የመገንዘብ እና ተገቢ ምላሽ የመስጠት፤ ➢ ምቹና ምቹ ባልሆነ ሁኔታ የሰዎችን ደረጃ፣ የስራ ሁኔታ፣ ወዘተ እንደ መመዘኛ ባለማስቀመጥ በብቃት ስራን የመስራት፣ የባህል እና ኢንተርፐርሰናል ልዩነቶችን የመቀበል፤ ➢ ግጭቶችና አለመስማማቶች ሲያጋጥሙ የተሳታፊዎቹ ስሜት እና ምላሽ መቆጣጠር በሚያስችል መንገድና በግለሰቦቹ የሚደርስ አሉታዊ ተፅእኖ በሚቀንስ አዎንታዊ በሆነ መንገድ የመፍታት እና ተገቢ የሆነ ድጋፍ የመስጠት ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ: VI

ዋና ዋና ተግባር እና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች /ስልጠና/
➢ ፈጠራና ግኝት በተሞላበት አካኋን የመፍትሄ ሃሳቦችን ያመነጫል፤ ➢ ማእቀፎችን ፣ ሞዴሎችንና አርክቴክቸሮችን ይነድፋል፤ ➢ ተቋማዊ የባህል ግንባታና የባህሪ ለውጥ ስትራቴጂዎችን፣ ሞዴሎችን፣ ፕሮግራሞችን፣ ማዕቀፎችን እና ካሪኩለሞችን ለማልማት አስፈላጊውን ሃገር አቀፍ ቅኝት ያከናውናል፣ ይመራል፤ ➢ ተቋማዊ የባህሪ ለውጥና የባህል ግንባታ ስትራቴጂዎችን፣ ሞዴሎችን፣ ሜተዶችን፣ ካሪኩለሞችን፣ ፕሮግራሞችን እና ማዕቀፎችን ያለማል፣	➢ ጥልቅ የዳሰሳና የዳሰሳ መንገዶች ዕውቀት፤ ➢ ችግሮችንና መፍትሄዎችን የመለየት፣የመጠቀም፤ ➢ ተቋማዊ የባህሪ/ባህል/ ለውጥ ማዕቀፎች/ሞዴሎች/ ስትራቴጂዎች/ስልቶች/ ሜተዶች ዲዛይን የማድረግ፤ ➢ ተቋማዊ ፍላጎቶች እና አጀንዳዎች፤ ➢ መፍትሄዎችን የመለየት፣ የመምረጥ፤ ➢ ያሉ የባህሪና ባህል ችግሮችን መረዳት፤ ➢ በሃገር ደረጃ አጀንዳዎችን፣ ጭብጦችንና ይዘቶችን ከኢላማዎች ጋር ማስተሳሰር መቻል፤ ➢ በሃገር ደረጃ ያሉ የባህሪ/ባህል/ ችግሮችን የመረዳት፤ ➢ በሃገር አቀፍ ደረጃ ያሉ የባህሪ/ባህል/ ለውጥ ግንባታ ችግሮችን የመለየት፣ የመረዳትና የመተንተን፤	➢ በሃገር ደረጃ ተፅእኖ መፍጠር የሚችል የባህሪ/ባህል/ ዳሰሳ የማከናወን ክህሎት፣ ➢ በዘርፉ የሚከናወኑ ዳሰሳዎች/ጥናቶች ዲዛይን የማድረግ ክህሎት፤ ➢ በሃገር ደረጃ ተፅእኖ መፍጠር የሚችል ጥናትና ዳሰሳ ዲዛይን የማድረግና የመምራት ክህሎት፤ ➢ በሃገር ደረጃ ትስስር የመፍጠር፤ ➢ በሃገር ደረጃ ተፅእኖ መፍጠር፤ ➢ የባህሪና ባህል ለውጥ/ግንባታ መፍትሄዎችን የመገምገም ክህሎት፣ ➢ በሃገር ደረጃ ተግባራዊ የሆኑ የባህሪ/ባህል ለውጥ/ግንባታ	የመጀመሪያ ወይም የሁለተኛ ዲግሪ በኮምፒተር ሳይንስ፣ በኮምፒዩተር ኢንጂነሪንግ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ ወይም ኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ ወይም በሳይኮሎጂ፣ በሶሺዮሎጂ እና በተመሳሳይ የሙያ ዘርፍ፤	➢ የመጀመሪያ ዲግሪ 8-10 ዓመት የስራ ልምድ፤ ➢ ሁለተኛ ዲግሪ 6-8 ዓመት የሥራ ልምድ	➢ CISAM (Certified Information Security Awareness Manager) ወይም ➢ MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program ወይም ➢ CSAP (Certified Security Awareness Practitioner) ወይም

	➢ መፍትሄዎችንና አማራጮችን የማመንጨትና ዲዛይን የማድረግ፤ ➢ የልማት (ዲዛይን) ዝርዝር ሂደቶችን የመረዳት፤	➢ መንደፍን ተግባራዊ የማድረግ ክህሎት፤ ➢ መፍትሄዎችን ዲዛይን የማድረግ ክህሎት፤ ➢ በሃገር ደረጃ የተፈጠረውን ተፅእኖ የመገምገም፣ ማስተካከያዎችን የመጠቆም ክህሎት፤ ➢ የክንውን መመዘኛ መስፈርቶችን የመቅረፅ ክህሎት፤ ➢ የስራ ክፍል ክንውኖችና ዝርዝር ተግባራት ዕቅድ የማውጣት ክህሎት፤ ➢ የሌሎችን ስራ አፈፃፀም መከታተል፣ የመገምገም፣ ሂስ የመስጠት ክህሎት፤		➢ PMP – Project Management Professional (ቢኖር ይመረጣል)

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ የማስፈፀም አቅም፤	➢ ተጨባጭ ሥራን መረዳት፣ መገንዘብና የማስፈፀም ችሎታ፤
➢ ተቋማዊ ዕውቀት፤	➢ ተልዕኮ ለመፈፀም ሥራ-ሂደትን፣ መመሪያዎችን፣ ሥራ መሳሪያዎችን የመጠቀም ችሎታ፤
➢ ችግር መፍታት፤	➢ ከፍተኛ የፈጠራ አካሄድ በመከተል ሥራን ማከናወን፤ ➢ በሃገር ደረጃ የሚታይ እሴት የመጨመር ብቃት እና በከፍተኛ ደረጃ ሌሎችን ማሳተፍ፤
➢ ተግባቦት፤	➢ ውጤታማ ቅንጅት (synergy) የመፍጠር ችሎታ፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ: VII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ በተሰማራበት ዘርፍ ስትራቴጂክ እቅድ ይቀርጻል፣ ይተገብራል፤ ➢ ተቋማዊ ፍላጎቶችንና የተሰማራበትን ምህዳር በጥልቅ በመረዳት አዝማሚያዎችን ያነባል፣ይተነትናል፣ እንዲሁም የአዝማሚያዎቹን ተጽእኖ ይተነብያል፤ ➢ በባህል ግንባታ ስትራቴጂዎች፣ ሞዴሎች፣ ካሪኩለሞች፣ ፕሮግራሞች እና ማዕቀፎች ልማት ዙሪያ ጥናቶችን ያካሄዳል፤ ➢ ተቋማዊ የባህሪ ለውጥ እና ባህል ግንባታ ስትራቴጂዎች፣ ሞዴሎች፣ ፕሮግራሞች እና ማዕቀፎችን ያለማል፤ ➢ በተቋም ደረጃ ተፅዕኖ የሚፈጥሩ አጀንዳዎችን፣ ጭብጦችንና ይዘቶችን ያለማል፤ ➢ የንቃተ ህሊና መመዘኛ ስታንደርዶችንና መንገዶችን ይቀርፃል፤ ➢ ተቋማዊ የንቃተ ህሊና ፕሮግራሞችን ያከናውናል፣ ያስተባብራል፤	➢ የመስኩ ሃገራዊ ፍላጎቶች እና አጀንዳዎች ዕውቀት፤ ➢ ተፈላጊ ባህሪ/ባህል/ የመቅረፅ ብቃት፤ ➢ የባህል/ባህሪ ለውጥ/ግንባታ ግቦችና አላማዎች የመቅረፅ፤ ➢ ስትራቴጂያዊ ጉዳዮችን ቅደም ተከተል (Prioritize) የማስያዝ፤ ➢ በሃገር አቀፍ ደረጃ የሚወጡ ልዩ ልዩ የባህሪ ለውጥ ሞዴሎች፣ ማዕቀፎች፣ ስትራቴጂዎች መስተጋብር መለየትና መረዳት፤ ➢ በሃገራዊ ኢንፎርሜሽን ደህንነት ባህሪ ለውጥና ባህል ግንባታ ዙሪያ የወቅታዊ ክንውኖች፣ ክስተቶች፣ስትራቴጂዎች፣ ሞዴሎች፣ ማዕቀፎች፣ ፕሮግራሞች፤	➢ በሃገር ደረጃ ተፅእኖ መፍጠር የሚችሉ የባህሪ/ባህል ለውጥ ማዕቀፎች፣ሞዴሎች፣ ስትራቴጂዎች፣ ስልቶች፣ ዲዛይን የማድረግ ክህሎት፤ ➢ በባህሪ/ባህል ለውጥ/ግንባታ ዙሪያ በሃገር ደረጃ የማማከር ክህሎት፤ ➢ መፍትሄዎችን ዲዛይን የማድረግ ክህሎት፤ ➢ በከፍተኛ ደረጃ የተሰሩ ስትራቴጂዎች፣ ሞዴሎች፣ ፕሮግራሞች፣ ማዕቀፎች፣ እና ካሪኩለሞች ታዳሚዎች በሚመጥን ደረጃ በፅሁፍ/በንግግር የማቅረብ ክህሎት፣ ➢ በከፍተኛ መጠን የስራ ክንውኖችን፣ ተግባሮችንና	➢ የመጀመሪያ ወይም ሁለተኛ ዲግሪ በኮምፒዩተር ሳይንስ፣ በኮምፒተር ኢንጂነሪንግ፣ በማናጅመንት ኢንፎርሜሽን ሲስተምስ፣ ኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ ወይም ➢ ሳይኮሎጂ፣ ሶሺዮሎጂ እና ተመሳሳይ የሙያ ዘርፍ፤	➢ የመጀመሪያ ዲግሪ 10-12 ዓመት የስራ ልምድ፤ ➢ ሁለተኛ ዲግሪ 8-10 ዓመት የሥራ ልምድ	➢ CISAM (Certified Information Security Awareness Manager) ወይም ➢ MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program ወይም ➢ CSAP (Certified Security Awareness Practitioner) ወይም

➢ በዘርፉ ያማክራል፣	➢ ስትራቴጂያዊ ቅደም ተከተል የማስያዝ፤ ➢ በየደረጃው የሚለሙ አጀንዳዎች፣ ጭብጦችና ይዘቶች ታዳሚዎችን በሚመጥን ሁኔታ የማቅረብ፤ ➢ ኢላማን በከፍተኛ መጠን የመገንዘብ፤	ሪፖርቶችን ስርአታዊ በሆነ መንገድ በፅሁፍና በንግግር የመግለፅ ክህሎት፣			➢ CISP (Certified Information Security Proffesional) ወይም ➢ CISM (Certified Information Security Manager) (ቢኖር ይመረጣል)

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅም	ማብራሪያ
➢ ስልታዊ ዕይታና የማስተሳሰር ብቃት፤	➢ ከፍ ብሎ ራስን ማየት መቻልና መሰረታዊ መርሆዎች ላይ ያነጣጠረ መማር የሚችል፤ እንዲሁም የላቀ ፈጠራ በታከለበት አካሄድ ስራን የማከናወን ብቃት፤ ➢ በተቋም ደረጃ የሚታይ እሴት የመጨመር ብቃት እና በከፍተኛ ደረጃ ሌሎችን ማሳተፍ፤
➢ ችግር መፍታት፤	➢ ተጨባጭ ሥራን መረዳት፣ መገንዘብና የማስፈፀም ችሎታ፣ ➢ ተልዕኮ ለመፈፀም ሥራ-ሂደትን፣ መመሪያዎችን፣ ሥራ መሳሪያዎችን የመጠቀም ችሎታ፤ ➢ ከፍተኛ የፈጠራ አካሄድ በመከተል ሥራ ማከናወን፤
➢ ተግባቦት፤	➢ ውጤታማ ቅንጅት (synergy) የመፍጠር ችሎታ፤
➢ ስብዕና፤	➢ ንቁነት፤ ➢ አንድ-ማንነት፤ ➢ አሳቢነት (Thinking)፤ ➢ የውስጥ ቁጥጥር (ከውስጥ ወደ-ውጭ የመመልከት)፤

የሥራ መደብ መጠሪያ፡ የሳይበር ደህንነት ንቃተ-ህሊና ባለሙያ

ደረጃ፡ VIII

ዋና ዋና ተግባር እና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራልምድ	ሰርተፍኬቶች
➢ በዘርፉ ፖሊሲና ስትራቴጂ እንዲቀረጽ ግብዓት ያሰባስባል፣ያሳምናል፤ ➢ በዘርፉ ተቋማዊ፣ አገራዊ እና አለም አቀፋዊ እይታዎችን ይቀርጻል፤ ➢ በአለም አቀፍ ደረጃ ተቀባይነት ያላቸው የባህል ግንባታ ስትራቴጂዎችን፣ ሞዴሎችን፣ ካሪኩለሞችን፣ ፕሮግራሞችን እና ማዕቀፎችን ያለማል፤ ➢ የባህል ግንባታና ባህሪ ለውጥ ስትራቴጂዎችን፣ ሞዴሎችን፣ ፕሮግራሞችን፣ ማዕቀፎችን እና ካሪኩለሞችን ለማልማት የሚያስችሉ ዲዛይኖችን፣ ሂደቶችንና ስርአቶችን ያለማል፤ ➢ በባህል ግንባታና በባህሪ ለውጥ ስትራቴጂዎች፣ ሞዴሎች፣ ማዕቀፎች እና ካሪኩለሞች ልማት ዙሪያ ጥናቶችን ያካሄዳል፣ የጥናት ፅሁፎችን ያሳትማል፤ ➢ በአለም አቀፍ ደረጃ ተቀባይነት ያላቸው የባህሪ ለውጥ ስትራቴጂዎችን፣ ሞዴሎችን፣ ካሪኩለሞችን፣ ፕሮግራሞችን እና ማዕቀፎችን ያለማል፤	➢ በአለም አቀፍ ደረጃ ተቀባይነት ያላቸው የባህሪ/ባህል/ ለውጥ ማዕቀፎች፣ሞዴሎች፣ ስትራቴጂዎችና ስልቶች ዲዛይን የማድረግ፤ ➢ የአለም አቀፋዊ አዝማሚያዎች እና ፍላጎት ዕውቀት፤ ➢ የግምገማ ስርዓት የመንደፍ ብቃት፣ ➢ ኢንዱስትሪ መሰረት ያደረጉ የአፈፃፀም አስተዳደር (መለኪያ) ሞዴሎች ስታንዳርድ የመለየት፣ የማወቅ እና አውዳዊ የማድረግ ብቃት፤ ➢ ግምገማዎች የመምራት እና በግምገማው ትምህርት የተወሰደባቸው አጠቃላይ ጉዳዮችን ቀምሮ የመሰነድ ብቃት፤ ➢ በአለም አቀፍ ደረጃ የሚወጡ ልዩ ልዩ የባህሪ	➢ በአለም አቀፍ ደረጃ ተፅእኖ መፍጠር የሚችል የባህሪ/ባህል/ ዳሰሳ የማከናወን ክህሎት፤ ➢ ችግሮችና መፍትሄዎችን የመለየትና የመጠቆም ክህሎት፤ ➢ አለም አቀፍ ተቀባይነት ያለው እና ተፅእኖ መፍጠር የሚችል የዳሰሳ ጥናት ዲዛይን የማድረግ፣ የመምራትና የማከናወን ክህሎት፤ ➢ በአለም አቀፍ ደረጃ በዳሰሳ ጥናት፣ በባህሪ/ባህል/ ለውጥ/ግንባታ/ ዙሪያ የማማከር ክህሎት፤ ➢ በአለም አቀፍ ደረጃ በባህሪ/ባህል/ ለውጥ/ግንባታ/ ዙሪያ ስልጠናዎችን	➢ የመጀመሪያ ወይም ሁለተኛ ዲግሪ በኮምፒዩተር ሳይንስ፣ በኮምፒዩተር ኢንጂነሪንግ፣ በማኔጅመንት ኢንፎርሜሽን ሲስተምስ፣ ኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ፤እንዲሁም ➢ በሳይኮሎጂ፣ በሶሺዮሎጂ እና በተመሳሳይ የሙያ ዘርፍ፤	➢ የመጀመሪያ ዲግሪ ከ12-14 ዓመት የስራ ልምድ፤ ➢ ሁለተኛ ዲግሪ ከ10-12 ዓመት የሥራ ልምድ	➢ CISAM (Certified Information Security Awareness Manager) ወይም ➢ CISP (Certified Information Security Profesional) ወይም ➢ CISM (Certified Information Security Manager) ወይም ➢ MGT433: SANS Security Awareness: How to

➢ በዘርፉ ያማክራል፤	ለውጥ ሞዴሎችን፣ ማዕቀፎችን፣ ስትራቴጂዎችን መስተጋብር የመለየትና የመረዳት ብቃት፤ ➢ በአለም አቀፍ ደረጃ በኢንፎርሜሽን ደህንነት የባህሪ ለውጥና የባህል ግንባታ ዙሪያ ወቅታዊ ክንውኖች፣ ክስተቶች እንዲሁም ስትራቴጂዎች፣ ሞዴሎች፣ ማዕቀፎችና ፕሮግራሞች ዕውቀት፤ ➢ በአለም አቀፍ ደረጃ ያሉ የባህሪ/ባህል/ ለውጥ/ግንባታ/ ችግሮችን የመለየት፣ የመረዳትና የመተንተን፤ ➢ በዘርፉ አለም አቀፍ የዕቅድና የሪፖርቲንግ ስርአቶች ዕውቀት፤	የመስጠት ክህሎት፤ ➢ ለውጥን የመቆጣጠር፣ የመከታተል ብቃት፤ ➢ አውቶሜትድ የግብረ-መልስ/ግምገማ/ ስርዓት የመንደፍ ክህሎት፤ ➢ መፍትሄዎችን ዲዛይን የማድረግ ክህሎት፤ ➢ አለም አቀፍ ደረጃውን በጠበቀ ሁኔታ የተሰሩ ስትራቴጂዎች፣ ሞዴሎች፣ ፕሮግራሞች፣ ማዕቀፎች እና ካሪኩለሞች ታዳሚዎችን በሚመጥን ደረጃ በፅሁፍ/በንግግር/ የማቅረብ ክህሎት፤ ✓ ኢላማን በከፍተኛ መጠን መገንዘብ፤			Build, Maintain, and Measure a Mature Awareness Program **ወይም** ➢ CSAP (Certified Security Awareness Practitioner) **ወይም** ➢ CGEIT (Certified in the Governance of Enterprise IT) **ወይም** ➢ GSLC: GIAC Security Leadership **ወይም** ➢ ISO risk management

					ወይም ➢ Information Security Awareness Foundational Assessment (ቢኖር ይመረጣል)

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ (Description)
➢ አለም አቀፋዊ ዕይታ፤	✓ አለም አቀፍና መጪውን የሳይበር ደህንነት ጉዳዮችን የመረዳት አቅም፤
➢ ስትራቴጂክ ዕይታ፤	✓ መጪውን የሳይበር ጥቃቶች ለመከላከል የሚያስችል አለም አቀፋዊ ስትራቴጂክ ዕይታ፤
➢ ችግር መፍታት፤	✓ ነባራዊ የሳይበር ደህንነት ችግሮች ተጨባጭ መፍትሄዎችን የማበልፀግ አቅም፤ ✓ በአለም አቀፍ ደረጃ የሚታይ እሴት የመጨመር ብቃት እና በከፍተኛ ደረጃ ሌሎችን ማሳተፍ፤
➢ ተግባቦት፤	✓ ከአለም አቀፍ የዘርፉ ባለሙያዎችና ተቋማት ጋር ትስስር የመፍጠር ብቃት፤

3.3. የሳይበር ደህንነት ኢንጂነሪንግ የሥራ ቡድን (ክፍል) መደቦች

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ: II

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ ድጋፍ እየተደረገለት የሳይበር ደህንነት ሲስተሞችን ጤንነት ይከታተላል፤ ➢ የሴክዩሪቲ ሪከርዶችን እና ዶክመንቶችን ይይዛል፤ ➢ የሴክዩሪቲ ኦፕሬሽን ማእከል ሲስተሞች ላይ በእገዛ ክትትል ያደርጋል፤ ➢ በተደራጀ አካባቢ ውስጥ መደበኛ እንቅስቃሴዎችን ያካሄዳል፤ ያልተጠበቁ ችግሮች ሲያጋጥሙ ድጋፍ ይጠይቃል፤	➢ አጠቃላይ ዕውቀት፤ ➢ የዳታ፣ አፕሊኬሽን፣ ኔትዎርክ እና end point security ጽንሰ ሃሳብ ዕውቀት፤ ➢ የኔትዎርኪንግ (Switching and routing) ዕውቀት፤ ➢ የሳይበር ሴክዩሪቲ ጽንሰ ሃሳብ ዕውቀት፤ ➢ የኦፕሬቲንግ ሲስተሞች መሰረታዊ ሴክዩሪቲ የማስተዳደር ዕውቀት፤	➢ የመግባባት ችሎታ፤ ➢ የተደራጀ ሥራ አቀራረብ ክህሎት፤ ➢ መሰረታዊ ስርዓቶችን እና መሳሪያዎችን፣ ትግበራዎችን እና ሂደቶችን የመጠቀም ክህሎት፤ ➢ የኦፕሬቲንግ ሲስተም ተከላ እና ኮንፊግሬሽን ክህሎት፤ ➢ መሰረታዊ የግል ደህንነት ልምድን የመረዳትና የመተግበር ክህሎት፤	➢ በኮምፕዩተር ሳይንስ፣ በኤሌክትሪካል ኢንጂነሪንግ ወይም በኢንፎርሜሽን ደህንነት የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ፤	➢ ለመጀመሪያ ዲግሪ ከ1-2 ዓመት አግባብነት ያለው የሥራ ልምድ፤ ለሁለተኛ ዲግሪ 0 ዓመት፤	

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ ስታንዳርዶችን፣ሞዴሎችን እና ማዕቀፎችን የመረዳትና የመተግበር ብቃት፤	➢ የተቀመጡ ስታንዳርዶችን፣ ሞዴሎችን እና ማዕቀፎችን ተከትሎ በእገዛ ሥራ ማከናወን፤ ➢ ስታንደርዶችን በመከተል የሚሰሩ ሥራዎችን መረዳት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ: III

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ የሳይበር ደህንነት ስጋት ትንተና ይተገብራል፤ ➢ የተቋሙን የሳይበር ደህንነት ፍላጎት ያስቀምጣል፤ ➢ የደህንነት ፍላጎትን መመለስ የሚችሉ የደህንነት ሰርቪሶችን ይለያል፤ የደህንነት ሰርቪሶችን ተግባራዊ ለማድረግ የሚያስችሉ ዘዴዎችን (mechanisms) እና ተስማሚ ቴክኖሎጂዎችን ለይቶ ይመርጣል፤ ➢ የዲዛይን መርሆችን ያስቀምጣል፤ ➢ የውስጥ ተጠቃሚዎችን የሲስተም አክሰስ እና ሲስተም ላይ የተሰሩ ስራዎችን ከሎግ በመነሳት አዲት ያደርጋል፤ ➢ የሴኩሪቲ ሪከርዶችን እና ዶክመንቶችን ይይዛል፤ ➢ የሴኩሪቲ አፕሬሽን ማእከል ሲስተሞች ላይ ክትትል ያደርጋል፤	➢ የደህንነት ፍላጎት ጽንሰ ሃሳብ ዕውቀት፤ ➢ የደህንነት ስጋት ትንተና ጽንሰ ሃሳብ ዕውቀት፤ ➢ የኢንፎርሜሽን እና ሳይበር ደህንነት ጽንሰ ሃሳብ ዕውቀት፤ ➢ የዳታ፣አፕሊኬሽን፣ ኔትዎርክ እና end point security ጽንሰ ሃሳብ ዕውቀት፤ ➢ የኔትዎርኪንግ (Switching and routing) ዕውቀት ፤ ➢ የደህንነት ኮንትሮሎች ምንነትና ጥቅም፤ ➢ መሰረታዊ የVulnerability assessment tools ዕውቀት፤ ➢ የደህንነት አርክቴክቸር ጽንሰ ሃሳብ ዕውቀት፤ ➢ የቴሌኮም አገልግሎቶች እና ኔትዎርክ ኮምፖነንቶች ዕውቀት፤	➢ የተለያዩ የስጋት ትንተና ስታንደርዶች ልዩነት እና አንድነት የማስቀመጥ፤ ➢ ስታንዳርዶችን ተከትሎ የስጋት ትንተና የማከናወን፤ ➢ የኦፕሬቲንግ ሲስተም ተከላ እና ኮንፊግሬሽን የማከናወን ክህሎት፤ ➢ የሲክዩሪቲ ቤዝላይን ግምገማ የመሥራት፤ ➢ ፕሮሲጀሮችን ተከትሎ የደህንነት ስጋት ትንተና የመስራት እና ግኝቶችን የመሰነድ፤	➢ በኮምፕዩተር ሳይንስ፣ በኤሌክትሪካል ኢንጂነሪንግ ወይም በኢንፎርሜሽን ደህንነት የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ፤	➢ ለመጀመሪያ ዲግሪ ከ2- 3 ዓመት ወይም ➢ ለሁለተኛ ዲግሪ 1 ዓመት አግባብነት ያለው የሥራ ልምድ	➢ Certification in routing and switching **ወይም** ➢ Certification in windows server, Unix/Linux and Solaris administration **ወይም** ➢ Certification in Security+ (ቢኖር ይመረጣል)

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ አፕሊኬሽን ሴክዩሪቲ የማረጋገጥ ብቃት፤	➢ የአፕሊኬሽን ደህንነት ኮንትሮሎችን ይለያል፣ ያወዳድራል፣ ይገመግማል፣ አማራጮችን ያቀርባል፣ሲፈቀድም ይተክላል፣ configuration ያሰራል፣ይፈትሻል፤ ➢ የአፕሊኬሽን ደህንነት ኮንትሮሎች ተከላ እንዲሁም configuration ያስተባብራል፤ ➢ የሚሰጠውን አቅጣጫ እና ማኑዋሎችን በመከተል የአፕሊኬሽን ሴክዩሪቲ ኮንትሮሎችን ይተክላል፣ configuration ይሰራል፤
➢ ኔትዎርክ ሴክዩሪቲ የማረጋገጥ ብቃት፤	➢ የኔትዎርክ ሲክዩሪቲ ዲዛይኖችን ያዘጋጃል፤ ➢ የኔትዎርክ ደህንነት ኮንትሮሎችን ይለያል፣ያወዳድራል፣ይገመግማል፣አማራጮችን ያቀርባል፣ሲፈቀድም ይተክላል፣ configuration ይሰራል፣ይፈትሻል፤ ➢ የኔትዎርክ ደህንነት ኮንትሮሎች ተከላ እና ኮንፊግሬሽን ማስተባበር፤ ➢ የሚሰጠውን አቅጣጫ እና ማኑዋሎችን በመከተል የኔትዎርክ ሲክዩሪቲ ኮንትሮሎችን ይተክላል፣ configuration ያደርጋል፤
➢ Vulnerability and penetration የመፈተሽ ብቃት፤	➢ የአፕሊኬሽን፣ የሲስተም እና የኔትዎርክ vulnerability እና penetration ፍተሻ መስራት፣ ሪፖርት ማዘጋጀት፤ ➢ የአፕሊኬሽን፣ የሲስተም እና የኔትዎርክ vulnerability እና የpenetration ፍተሻ ሥራ ማገዝ፤
➢ System የማጠንከር ብቃት፤	➢ የአሰራር ማኑዋሎችን ተከትሎ የአፕሊኬሽን እና የኔትዎርክ ማጠንከር (hardening) ሥራ መስራት፤ ➢ የፓች ማናጅመንት ሥራ መስራት፤ ➢ የአፕሊኬሽን እና የኔትዎርክ ማጠናከር (hardening) ሥራ ማገዝ፤

የሥራ መደብ: የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ: IV

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ ሞዴሎችንና ማዕቀፎችን ይመርጣል፤ የdefense-in-depth መርህን መሠረት ያደረገ እና ተግባራዊ ሊሆን የሚችል ሁሉን አቀፍ የደህንነት አርክቴክቸር ይነድፋል፤ ➢ ለተመረጡ ቴክኖሎጂዎች ስፔሲፊኬሽን ያዘጋጃል፤ እንዲሁም የሚገኙበትን ስትራቴጂ (በግዢ፣ በማልማት ወይም ያሉትን በመጠቀም) ያስቀምጣል፤ ➢ ቴክኖሎጂዎች በስፔስፊኬሽኑ መሠረት መቅረባቸውን ያረጋግጣል፤ ➢ በተቋሙ ውስጥ ወደሚገኙ ማናቸውም ሲስተሞች ለመግባት የሚቀርቡ ጥያቄዎችን በተቋሙ ፖሊሲ መሰረት ይቆጣጠራል፤ ይፈቅዳል፤ ➢ የተቋሙን የሳይበር ደህንነት ኢንጂነሪንግ ፕሮጀክት ያስተባብራል፤ ያስተዳድራል፤	➢ የደህንነት ፕሮጀክቶችን የመገምገምያ ዘዴዎች ዕውቀት፤ ➢ የደህንነት ስጋት ትንተና ማዕቀፎችና ስታንዳርዶች የመገምገሚያ ዘዴዎች ዕውቀት፤ ➢ የደህንነት አርክቴክቸር መንደፊያ ማዕቀፎች ወቅታዊ ሁኔታ ዕውቀት፤ ➢ ወቅታዊ የደህንነት ስጋት እና የመከላከያ ዘዴዎች ዕውቀት፤ ➢ የደህንነት አርክቴክቸር መንደፊያ ማዕቀፎች ዕውቀት፤ ➢ የሞዴሎች፣ማዕቀፎችና ስታንዳርዶች ዝግጅት ዕውቀት፤ ➢ ቴስት ኬዞችን የማዘጋጀት ዕውቀት፤	➢ የደህንነት ፕሮጀክቶችን የመምራት እና የመገምገም ክህሎት፤ ➢ ደረጃውን የጠበቀ የስጋት ትንተና የማከናወን ክህሎት፤ ➢ የደህንነት መቆጣጠሪያዎችን የማዘጋጀት፣የመገምገም እና በቂ ማብራሪያ የመስጠት ክህሎት፤ ➢ ደረጃውን የጠበቀ የደህንነት አርክቴክቸር የመንደፍ እና የመገምገም ክህሎት፤ ➢ ስታንዳርዶችን ተከትሎ የደህንነት ፍላጎቶችን የመለየት እና የመግለጽ ክህሎት፤ ➢ የተለያዩ የደህንነት መቆጣጠሪያዎችን ማስማማት እና የመሞከር ክህሎት፤ ➢ የደህንነት አቋምን ከስታንዳርዶች አንጻር	➢ በኮምፕዩተር ሳይንስ፣ በኤሌክትሪካል ኢንጂነሪንግ ወይም በኢንፎርሜሽን ደህንነት የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ፤	➢ ለመጀመሪያዲግሪ ከ3-4 ዓመት ➢ ለሁለተኛ ዲግሪ 1- 2 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Ceritification in identity and access mangement systems **ወይም** ➢ Certification on Enterprise security architecture design (like SABSA (Sherwood Applied Business Security Architecture)) **ወይም** ➢ Certified Information Systems Security Professional (CISSP) **ወይም** Certified Information Security Manager

		የመሠረታዊ ክህሎት፤ የማስተካከያ ሥራዎችን የመሥራት ክህሎት፤ ➢ ለጥቃት የሚውሉ ቴክኖሎጂዎች እና የተዘጋጀው ስፔሲፊኬሽን የማረጋገጥ ክህሎት፤ ➢ የተጋላጭነት ጳሰና የስርጎ ገብ መከራ የመለየት ክህሎት፤ ➢ ኦፕሬሽናል እና troubleshooting ሥልጠናዎች የመስጠት ክህሎት፤			(CISM) (ሊኖር ይመረጣል)፤

የሥራ መደቡ መጠሪያ: የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ: V

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ በአርክቴክቸር ላይ የተቀመጡትን ኮምፖነንቶች ይተክላል፤ ➢ እያንዳንዱ ኮምፖነንት በአግባቡ መሰራቱን ይፈትሻል፣ እርስ በእርስ መናበባቸውን እና በመካከላቸው ያለውን የዳታ ፍሰት ትክክለኛነት ያረጋግጣል፤ ➢ የተቋሙን አዲስ የቢዝነስ ፕሮፖዛል ይገመግማል፤ በሴክዩሪቲ ጉዳዮች ላይ ሙያዊ ምክሮችን ይሰጣል፤ ➢ ደረጃቸውን የጠበቁ የኦፕሬሽን መመሪያዎችን እና troubleshooting ማኑዋል ያዘጋጃል፣ ይሰንዳል፤ ➢ ተቋማዊ የሳይበር ደህንነት ፖሊሲዎችን ለባለሙያዎች ያሳውቃል፣ተግባራዊታቸውን ይከታተላል፤ ➢ ለተጠቃሚዎች የኦፕሬሽናል እና የጥገና ሥልጠና ይሰጣል፤ ➢ የተቋሙን ፍላጎት መመለስ በሚችል መልኩ ሲስተም መተከሉን እና ለአገልግሎት መዘጋጀቱን ያረጋግጣል፤ ➢ የሳይበር ደህንነት ኢንጂነሪንግ ፕሮጀክቶች በሃገራዊ የሳይበር	➢ የሃገራዊ የሳይበር ደህንነት ፖሊሲዎች፣ ስትራቴጂዎች እንዲሁም ዘርፉን የሚመለከቱ ህጎች ዕውቀት፤ ➢ የደህንነት ስጋት ትንተና ማዕቀፎችን ማላመጃ ዘዴዎችና ወቅታዊ ዓለም አቀፍ ልምዶች ዕውቀት፤ ➢ የደህንነት አርክቴክቸር መንደፊያ ማዕቀፎች የማላመጃ ዘዴዎች ዕውቀት፤ ➢ የሞዴሎችና ማዕቀፎች ዝግጅት ዕውቀት፤	➢ ወቅታዊ የስጋት ሁኔታን የሚያሳዩ ጽሁፎች ማዘጋጀት፤ ➢ በተቋሙ የተተገበሩ ፕሮጀክቶች ያመጡትን ተጽእኖዎች የመገምገም እና የመሰነድ፤ ➢ የደህንነት ኮንትሮሎችን ስፔሲፊኬሽን በማዘጋጀት ጥናትና ምርምር ወይም የማበልጸግ ሥራን የመምራት፤ ➢ ወቅታዊ የደህንነት ኮንትሮሎችን የመከታተል፣የመሰነድ፣ በቂ ማብራሪያ የመስጠት፤ ✓ ሞዴሎችን፣ ፍሬምዎርኮችን፣ ስታንዳርዶችን አዶፕት የማድረግ ክህሎት፤	➢ በኮምፕዩተር ሳይንስ፣ በኤሌክትሪካል ኢንጂነሪንግ በኢንፎርሜሽን ደህንነት የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ	➢ ለመጀመሪያ ዲግሪ ከ4 እስከ 5 ዓመት ➢ ለሁለተኛ ዲግሪ 2 እስከ 3 ዓመት አግባብነት ያለው የሥራ ልምድ	➢ Ceritification on identity and access mangement systems ወይም ➢ Certification on Vulnerability assessment and penetration testing ወይም ➢ Certified Information ወይም ➢ Security Manager (CISM) ወይም ➢ ITIL 4 Foundation Level ቢኖር ይመረጣል፤

ደህንነት ፖሊሲዎች እና ማዕቀፎች መሰረት መሰራታቸውን ያረጋግጣል፤ ➢ የተቋሙ የሳይበር ደህንነት ስርዓቶች ከሃገራዊ ሳይበር ደህንነት ስርዓት ጋር ተናባቢ እንዲሆኑ ከሚመለከታቸው ባለድርሻዎች ጋር ይወያያል፤					

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የፕሮጀክት አመራር ብቃት፤	➢ አስፈላጊ መርሆችን እና ተሞክሮዎችን ከፕሮጀክቱ ግብ አንጻር የጋራ ምርታማነትን የሚጨምሩ ተግባርና ሃላፊነት ከግንዛቤ በማስገባት ባለድርሻ አካላትን በማሳተፍ መምራት፤
➢ የኔትዎርክ እና ደህንነት ቴክኖሎጂዎችን የመትከል እና የመፈተሽ ብቃት፤	➢ የሚሰጠውን አቅጣጫ እና ማኑዋሎችን ተከትሎ የኔትዎርክ እና ደህንነት ቴክኖሎጂ ኮንፊግሬሽንና የፍተሻ ሥራ መስራት፤ ➢ በደህንነት አርክቴክቸር ላይ የተቀመጡ የኔትዎርክ እና ደህንነት መቆጣጠሪያዎች ላይ ሃሳብ መስጠት፣ አማራጮችን ማቅረብ፣ በግምገማ ሂደት መሳተፍ፣ መትከል፣ የኮንፊግሬሽን ሥራ ማከናወን፣ መፈተሽ፣ አዳዲስ ቴክኖሎጂዎችን መትከልና መሰነድ፤

የሥራ መደቡ መጠሪያ፡- የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ፡- VI

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ የተቋሙን ግቦችንና ሂደቶችን ለማሟላት በሚያስችል መልክ የራሱን ዕቅድ ያወጣል፤ ➢ በፕሮጀክቶች ደንበኞችን፣ አቅራቢዎችን እና አጋሮችን ይከታተላል፤ ➢ ዒላማዎች ስኬት ላይ ተጽዕኖ የሚያሳድሩ ውሳኔዎችን ይሰጣል፤ ➢ ከቡድን አባላት፣ ከተጠቃሚዎች እና ከደንበኞች ጋር በመደበኛነት ይሠራል፤ ➢ የተጠቃሚ ፍላጎቶች መሟላታቸውን ያረጋግጣል፤ ➢ በተለያዩ ሁኔታዎች ውስጥ በርካታ ውስብስብ ቴክኒካዊ ወይም የባለሙያ እንቅስቃሴዎችን ያጠቃልላል፣ ውስብስብ ጉዳዮችን ይመረምራል፣ ያብራራል እንዲሁም ይፈታል፤	➢ የሃገራዊ የሳይበር ደህንነት ፖሊሲዎች፣ ስትራቴጂዎች እንዲሁም ዘርፉን የሚመለከቱ ህጎች ዕውቀት፤ ➢ የደህንነት ስጋት ትንተና ማዕቀፎችን ማላመጃ ዘዴዎችና ወቅታዊ ዓለም አቀፍ ልምዶች ዕውቀት፤ ➢ የደህንነት አርክቴክቸር መንደፊያ ማዕቀፎች የማላመጃ ዘዴዎች ዕውቀት፤ ➢ የሞዴሎችና ማዕቀፎች ዝግጅት ዕውቀት፤	➢ በንግግር እና በፅሁፍ ሀሳቡን በሰላ መንገድ የማስተላለፍ፤ ➢ ውስብስብ ጉዳዮችን ቴክኒካዊ እና ቴክኒካዊ ላልሆኑ ሰዎች የማቅረብ፤ ➢ ዕቅዶችን፣ መርሃግብሮችን፣ የቁጥጥር ጊዜዎችን እና የጥራት ግቦችን ለማሳካት የሚያስችሉ ጉዳዮችን የማስቀመጥ፤ ➢ አዲስ መረጃን በፍጥነት ይቀበላል እና ውጤታማ በሆነ መንገድ የመተግበር ክህሎት፤ ➢ የጋራ ዓላማዎችን በሚጋሩ ባለድርሻ አካላት መካከል ትብብር የማመቻቸት፤ ➢ ትክክለኛ የሆኑ ደረጃዎች፣ ዘዴዎች፣ መሣሪያዎች እና መተግበሪያዎች የመምረጥ፤	➢ በኮምፕዩተር ሳይንስ ወይም በኤሌክትሪካል ኢንጂነሪንግ ወይም በኢንፎርሜሽን ደህንነት፤ የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ	➢ ለመጀመሪያ ዲግሪ ከ5 እስከ 6 ዓመት፤ ➢ ለሁለተኛ ዲግሪ 3 እስከ 4 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Ceritification on identity and access mangement systems **ወይም** ➢ Certification on Enterprise security architecture design (like SABSA (Sherwood Applied Business Security Architecture)) **ወይም** ➢ Certification on Vulnerability assessment and penetration testing **ወይም** ➢ Certified Information Systems **ወይም** ➢ ITIL 4 Foundation Level ቢኖር ይመረጣል፤

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የፕሮጀክት አመራር ብቃት፤	➢ አስፈላጊ መርሆዎችን እና ተሞክሮዎችን ከፕሮጀክቱ ግብ አንጻር የጋራ ምርታማነትን የሚጨምሩ ተግባርና ሃላፊነቶችን ከግንዛቤ በማስገባት ባለድርሻ አካላትን በማሳተፍ መምራት፤
➢ የኔትዎርክ እና ደህንነት ቴክኖሎጂዎችን የመትከል እና የመፈተሽ ብቃት፤	➢ የሚሰጠውን አቅጣጫ እና ማኑዋሎችን ተከትሎ የኔትዎርክ እና ደህንነት ቴክኖሎጂ ኮንፊግሬሽንና የፍተሻ ሥራ መስራት፤ ➢ በደህንነት አርክቴክቸር ላይ የተቀመጡ የኔትዎርክ እና ደህንነት ኮንትሮሎች ላይ ሃሳብ መስጠት፣ አማራጮችን ማቅረብ፣ በግምገማ ሂደት መሳተፍ፣ መትከል፣ የኮንፊግሬሽን ሥራ ማከናወን፣ መፈተሽ፣ አዳዲስ ቴክኖሎጂዎችን መትከል እና መሰነድ፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ: VII

ዋና ዋና ተግባር እና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራልምድ	ሰርተፍኬቶች
➢ የቴክኒካል፣ የፋይናንስ እና የጥራት ገጽታዎችን ጨምሮ በአንድ ወሳኝ የሥራ መስክ ውስጥ ለሚከናወኑ እርምጃዎች እና ውሳኔዎች ስልጠና ይሰጣል፤ ➢ ኢንዱስትሪ መሪዎችን ጨምሮ ከውስጥ እና ከውጭ ደንበኞች፣ ከአቅራቢዎች እና ከአጋር አካላት ጋር ግንኙነቶች ይፈጥራል፤ ➢ የተቋሙ ዒላማዎች እና በፋይናንስ አፈፃፀም ላይ ተጽዕኖ ያላቸውን ውሳኔዎችን ይሰጣል፤ ➢ የቴክኒካዊ፣ የፋይናንስ እና የጥራት ገጽታዎችን ለሚሸፍን የሚረዱ የሥራ እንቅስቃሴዎችን ያካሄዳል፤ ➢ ለተቋሙ ፖሊሲ እና ስትራቴጂ ትግበራ አስተዋጽ ያደርጋል፤ ➢ ሰፋ ያሉ ቴክኒካዊ እና/ወይም የአስተዳደር መርሆዎችን በፈጠራ ይተገበራል፤	➢ በድርጅት ውስጥ አጠቃላይ እና የተወሰኑ አተገባበር ዕውቀት ይኖረዋል፤ ➢ የዳበረ የድርጅት፣ የአቅራቢዎች፣ የአጋሮች፣ የተወዳዳሪዎች እና የደንበኞች እንቅስቃሴ የንግድ ሥራ ዕውቀት፤ ➢ የተቋሙ አሰራር ላይ መሰረታዊ ዕውቀት፤	➢ ግልጽ አመራር የመስጠት፤ ➢ በሁሉም ደረጃዎች ውጤታማ በሆነ መልኩ ለቴክኒክና ቴክኒካዊ ላልሆኑ ሃሳብ በግልጽ የማስተላለፍ፤ ➢ የአዳዲስ የቴክኖሎጂ አንድምታዎችን የመረዳት፣ ➢ በተቋም ውስጥ የቴክኖሎጂን ሚና እና ተፅእኖ የመረዳትና ለሌሎች የማስተላለፍ፤ ➢ የተወሳሰቡ መረጃዎችን የመፍታት፤ ➢ ከተለያዩ ሀገች ጋር የተጣጣሙ ማዕቀፎች እና ስምምነቶች	➢ በኮምፕዩተር ሳይንስ ፣ በኤሌክትሪካል ኢንጂነሪንግ፣ በኢንፎርሜሽን ደህንነት የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ ፤	➢ ለመጀመሪያ ዲግሪ ከ6 እስከ 7 ዓመት፤ ➢ ለሁለተኛ ዲግሪ 4 እስከ 5 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Certified Information Systems Security Professional (CISSP) **ወይም** ➢ Certified Information **ወይም** ➢ Security Manager (CISM) **ወይም** ➢ ITIL 4 Strategic Leader (SL) ቢኖር ይመረጣል፤

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ የሳይበር ደህንነት ምህንድስና ስራዎች በተቋሙ ውስጥ በአግባቡ እንዲከናወኑና ተቀባይነት እንዲያገኙ የማሳመን እና ተጽእኖ የመፍጠር ብቃት፣
➢ የአመራር ብቃት፤	➢ የተቋሙን የሳይበር ደህንነት ምህንድስና ስራ አመራር ተቋሙ በሚያስቀምጣቸው ህጎች፣ መመሪያዎች፣ ፍልስፍናዎች እና ደንቦች መሰረት የመምራት፣ የመከታተልና የመመዘን ብቃት፤
➢ የደህንነት ስጋት የመገምገም ብቃት፤	➢ የተለያዩ ስታንዳርዶችን፣ ዘዴዎችን እና መሳሪያዎችን በመጠቀም የደህንነት ስጋት ግምገማ መተግበርና የምላሽ ስትራቴጂ ማስቀመጥ፤

የሥራ መደቡ መጠሪያ፡- የሳይበር ደህንነት ኢንጂነሪንግ ባለሙያ

ደረጃ፡- VIII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ ለተቋሙ ተልዕኮ ስኬት በዘርፉ ቁልፍ የሆኑ ውሳኔዎችን ይሰጣል፤ ➢ በተቋሙና ከተቋሙ ተልዕኮ ጋር ተያያዥነት ባላቸው ዘርፎች መካከል የቴክኖሎጂ እውቀትን እና/ወይም/ ግኝቶችን ያሻሽላል፤ ➢ ከደንበኞች፣ ከአጋሮች፣ ከኢንዱስትሪ መሪዎች እና ከመንግስት ጋር የረጅም ጊዜ ስትራቴጂክና ስልታዊ ግንኙነቶች ያዳብራል፤ ➢ የስትራቴጂክ አወጣጥን እና አተገባበርን ይመራል፤ ➢ በዘርፉ የሚኖሩ ተግባራትን በአግባቡ በመምራት በከፍተኛ ደረጃን ይተገበራል፤	➢ ከተቋሙ እንቅስቃሴዎች እና ልምዶች መነሻ የአቅራቢዎችን፣ የአጋሮችን፣ የተወዳዳሪዎችን እና ደንበኞችን ፍላጎት በጥልቀት ማወቅ፤ ➢ በተቋሙ ተጽዕኖ በሚያሳድሩ አካባቢዎች ስትራቴጂክና ስልታዊ የአመራር ዕውቀት፤ ➢ በተቋሙ ተልዕኮ አፈጻጸም ተጽዕኖ የሚያሳድሩ ጉዳዮችን በጥልቀት የማወቅና የመተግበር፤	➢ ሙሉ ስትራቴጂካዊ የአመራር ችሎታ፤ ➢ በድርጅቶች እና በግለሰቦች ላይ ያሉ አዳዲስ ልምምዶች እና ቴክኖሎጂዎች ያላቸውን ተፅእኖ የማስተላለፍ፤ ➢ ያሉትን ልምዶች እና ቴክኖሎጂዎች የመጠቀም ወይም ያለመጠቀም አደጋዎችን የመገምገም፤ ➢ አሳማኝ በሆነ መንገድ በሁሉም ደረጃዎች ውስብስብ ሃሳቦችን በሚገባ የመረዳት፣ ➢ የማብራራት እንዲሁም ለሌሎች የማቅረብ፤ ➢ የሕግ ተጽዕኖና አካታችነቱ የመገምገም፣ ➢ ዘርፉ የሚያስፈልጉትን ሙያዎችና ችሎታዎች ሙሉ በሙሉ ማዳበሩንና ማደራጀቱን ለማረጋገጥ የሚያስችል ብቃት፡	➢ በኮምፕዩተር ሳይንስ ወይም በኤሌክትሪካል ኢንጂነሪንግ ወይም በኢንፎርሜሽን ደህንነት የመጀመሪያ ዲግሪ ወይም የሁለተኛ ዲግሪ፤	➢ ለመጀመሪያ ዲግሪ ከ7 እስከ 9 ዓመት ➢ ለሁለተኛ ዲግሪ 5 እስከ 7 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Certified Information Systems Security Professional (CISSP) ወይም ➢ Certified Information Security Manager (CISM) ወይም ➢ ITIL Master Certificatation ቢኖር ይመረጣል፤

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ የሳይበር ደህንነት ምህንድስና ስራዎች በተቋሙ ውስጥ በአግባቡ እንዲከናወኑና ተቀባይነት እንዲያገኙ የማሳመን እና ተጽእኖ የመፍጠር ብቃት፣
➢ የአመራር ብቃት፤	➢ የተቋሙን የሳይበር ደህንነት ምህንድስና ስራ አመራር ተቋሙ በሚያስቀምጣቸው ህጎች፣ መመሪያዎች፣ ፍልስፍናዎች እና ደንቦች መሰረት የመምራት፣ የመከታተልና የመመዘን ብቃት፤
➢ የደህንነት ስጋት የመገምገም ብቃት፤	➢ የተለያዩ ስታንዳርዶችን፣ ዘዴዎችን እና መሳሪያዎችን በመጠቀም የደህንነት ስጋት ግምገማ መተግበርና የምላሽ ስትራቴጂ ማስቀመጥ፤

3.4. የሳይበር ደህንነት ኦዲት እና ግምገማ ቡድን (ክፍል) የሥራ መደቦች

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ

ደረጃ: I

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ በተሰጠው ፖሊሲ፣ ደንብ እቅድ እና ወሰን መሰረት መረጃ ይሰበስባል፤ ከፍተቶችን ይለያል፤ ➢ በተሰጠው የስራ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያስቀምጣል፤ ➢ ለኦዲቲንግ ክዋኔ የሚያስፈልጉ መረጃዎችን ይሰበስባል፤ ➢ በቅርብ ክትትል በተሰጠው ኢላማ (Target) መሰረት ክፍተትን ራስ ሰር (automated) መተግበሪያዎችን በመጠቀም የመለየት ስራ ይሰራል፤ ➢ የተገኙ ክፍተቶችን ሪፖርት ያደርጋል፤	➢ የኢንፎርሜሽን ኮምኒኬሽን ሲስተሞች፣ አፕሊኬሽንኖች እና ስርዓቶችን የመረዳት፤ • ስርዓተ ክወናዎች (operating system)፣ የመረጃ ቋት አፕሌኬሽን (መተግበሪያ) እና የድር መድረኮች (web platforms) ዕውቀት፤ • የኮምፒውተር ትስስር (computer networks) እና የትስስር ፕሮቶኮሎች እና አገልግሎቶች ዕውቀት፤ ➢ የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ደህንነት ግንዛቤ፤ ➢ የመረጃ መሰብሰቢያ መሳሪያዎች፣ የአሰራር ዘዴዎች፤ ➢ የኦዲት መረጃ መሰብሰቢያ መንገዶችና መሳሪያዎች፤ ➢ ራስ-ሰር (automated vulnerability assessment) መተግበሪያዎችን ማወቅ እና	➢ ለደህንነት ምዘና የሚረዱ መረጃዎችን መለየት መቻል፤ ➢ መረጃ ለማደራጀት የሚችሉ መተግበሪያዎችን መጠቀም መቻል፤ ➢ የደህንት ክፍተት ለመለየት የሚያገለግሉ መተግበሪያዎችን በመጠኑ መጠቀም መቻል፤	በኢንፎርሜሽን ሳይንስ፣ኮምፒውተር ሳይንስ፣ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ዲግሪ፤	የመጀመሪያ ዲግሪ 0-1 ዓመት፣	

	በቴክኖሎጂ የተደገፈ ተጋላጭነትን የመለየት ዕውቀት፤				
የመወዳደሪያ አቅሞች	**ማብራሪያ**				
➢ መረጃን ማሰባሰብ፤	➢ የሳይበር ደህንነት አዲት እና ግምገማው የሚከናወንበት ሒላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤				
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤				

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ
ደረጃ: II

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ስርተፍኬት
➢ በደረጃ 1 ባሉ ባለሞያዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ በደረጃ 1 የተሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ያረጋግጣል፤ ➢ በተሰጠው የስራ እቅድ መሰረት የራሱ እቅድ እና አተገባበር ሂደት ያስቀምጣል፤ ➢ በተሰጠው ወሰን መሰረት እሴቶችን ይለያል፣ ያደራጃል፣ እና የሙከራ ቅደም ተከተል ያወጣል፤ ➢ ራስ-ሰር መተግበሪያዎችን በመጠቀም በተሰጠው የአሰራር ሂደት መሰረት ክፍተቶችን ይለያል፤ ይተነትናል፤ ➢ ራስ ሰር መተግበሪያዎችን በመጠቀም የአፈጻጸም አቅምን በተቀመጠለት መስፈርት መሰረት	➢ እሴት የመለየት እና የመከፋፈል እውቀት፤ ➢ ራስ-ሰር (automate) በቴክኖሎጂ የተደገፈ የተጋላጭነት ትንተና ዕውቀት፤ ➢ የአፈጻጸም ደረጃን የመለካት እውቀት፤ ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች እውቀት፤ ➢ የሳይበር ደህንነት፣ ሲስተምና መሰረተ ልማት የመገንዘብ፤	➢ እሴቶችን በተሰጠው ወሰን መሰረት መለየት እና እንደ ባህሪያቸው የመከፋፈል፤ ➢ የስርዓት ሙከራ ተግባቢነት (compatibility) እና የአፈጻጸም (performance testing) ሙከራ የማካሄድ፤ ➢ ክፍተቶችን ለመለየት የሚጠቅሙ መተግበሪያዎችን በተፈለገው ደረጃ የመጠቀም፤	በኢንፎርሜሽን ሳይንስ፣ኮምፒውተር ሳይንስ፣ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ዲግሪ ወይም ሁለተኛ ዲግሪ፤	➢ የመጀመሪያ ዲግሪ ከ1 እስከ 2 ዓመት አግባብነት ያለው የሥራ ልምድ ወይም ➢ ሁለተኛ ዲግሪ 0 ዓመት፤	

ይመዘናል(Performance Testing)፤ ➢ ራስ ሰር መተግበሪያዎች የሚያስቀምጧችውን ምክር ሃሳቦች ክፍተቶቹ አንጻር ተንትኖ ያስቀምጣል፣ ➢ የተገኙ ክፍተቶችን ሪፖርት ያደርጋል፤					
የመወዳደሪያ አቅሞች	**ማብራሪያ**				
➢ መረጃን ማሰባሰብ፤	➢ የሳይበር ደህንነት አዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤				
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የአዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤				

የሥራ መደብ መጠሪያ ፡ የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ

ደረጃ፡ III

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ይመራል፤ ያበቃል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ➢ በተሰጠው የስራ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያስቀምጣል፤ ➢ በራስ ሰር መተግበሪያዎች የተገኙ ክፍተቶችን ሐሰት አዎንታዊ (false positive) ውጤቶችን ይለያል፤ ➢ የታውቁ ክፍተቶችን የሰርጎ ገብ (know vulnerability exploitation) ሙከራ ያካሄዳል፤	➢ ራስ ሰር መተግበሪያዎችን በጥልቀት የመረዳት፣ ➢ ራስ ሰር መተግበርያዎች በሚሰጡት ውጤት መሰረት ሐሰት አወንታዊ የመለያ መንገዶችን ማወቅ፤ ➢ ሰርጎ ገብ መተግበሪያዎችን የመረዳት እና እንደ ባህሪያቸው የመተግበር እውቀት፤ ➢ ደህንነታቸው የተጠበቁ መተግበሪያዎችን የማበልጸግ እውቀት እና የደህንነታቸውን ደረጃ ለመገምገም የሚጠቅሙ የራስ ሰር መተግበሪያዎች፤ ➢ የሶርስ ኮድ እና የኢቴኮ ደህንነት መቆጣጠሪያዎችን እና መንገዶችን ማወቅ፤ ➢ የስጋት ሞዴልን መሰረት በማድረግ የደህንነት ፍተሻ የማድረግ እውቀት፤ ➢ የአፈጻጸም አቅምን ለመለካት የሚያስችል እና የመመዘኛ	➢ ሐሰት አዎንታዊ ውጤቶችን የተለያዩ ዘዴዎችን በመጠቀም መለየት፤ ➢ የታወቁ ክፍተቶች የሰርጎ ገብ መከራ የማካሄድ ክህሎት፤ ➢ የሶርስ ኮድ ክፍተቶችን ለመለየት የሚያስችሉ መተግበሪያዎችን መጠቀም መቻል፤ ➢ የስጋት ሞዴልን የመረዳት እና በዚያም መሰረት ምዘና የማካሄድ፤ ➢ ተጨባጭ እና ከክፍተቱ ጋር ተመጣጣኝ የሆነ ምክረ ሃሳብ የማቅረብ፤ ➢ የስርዓት መከራ ተግባቢነት(compatiblity) ጭነት፣ ውጥረት	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ዲግሪ ወይም ሁለተኛ ዲግሪ	➢ የመጀመሪያ ዲግሪ ከ2 እስከ 3 ዓመት ወይም ➢ ሁለተኛ ዲግሪ 0 እስከ 1 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Information Security ወይም ➢ Vulnerability scanning ወይም ➢ Secure appliation developmemt and application security ቢኖር ይመረጣል፤

➢ በራስ ሰር መተግበሪያዎች በመጠቀም የሶርስ ኮድ አዲት ያካሄዳል፤ ➢ ለተረጋገጡ ክፍተቶች እና የሶርስ ኮድ አዲት ክፍተቶች ምክረ ሃሳቦችን ያስቀምጣል፤ ➢ ከኢላማው እና ከኢላማው የደህንነት መስፈርቶች እና ከተሰጠው የስጋት (threat) ሞዴል በመነሳት የደህንነት መጠበቂያ ተግባራትን (security functionality) ሙከራ ያካሄዳል፤ ➢ ራስ ሰር መተግበሪያዎችን በመጠቀም የአፈጻጸም አቅምን ለመለካት የሚውል መስፈርት ያዘጋጃል፤ ➢ የተገኙ ክፍተቶችን ሪፖርት ያደርጋል፤	መንገዶችን እና ደረጃዎችን በጥልቅት ማወቅ፤	እና የአፈጻጸም ሙከራ (performance testing) የሚሆኑ መስፈርቶችን ከምርጥ ተሞክሮ እና ከኢላማው በመነሳት የማበልጸግ ክህሎት፤			

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ መረጃን ማሰባሰብ፤	➢ የሳይበር ደህንነት አዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ

ደረጃ: IV

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ይመራል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ➢ በተሰጠው የስራ እቅድ መሰረት የራሱ እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ የሰው ኃይል የመረጃ ደህንነት ንቃተ ህሊናን ይመዝናል ፤ ➢ የሰርጎ ገብ መተግበሪያዎችን ለኢላማው በሚሆን መልኩ ያበጃል (exploit customization)፤ ➢ የሶርስ ኮድ ኦዲት በራስ	➢ የሰው ኃይል የደህንነት ንቃተ ህሊና አተገባበር፣ የምዘና መንገዶች እና መተግበሪያዎች ዕውቀት፤ ➢ የማህበራዊ ምህንድስና (Social-Engineering) ዕውቀት፤ ➢ የሰርጎ ገብ መተግበሪያዎች አሰራር ሂደቶች፣ ስክሪፕቶች እና ባህሪ አረዳድ ዕውቀት፤ ➢ የሶርስ ኮድ ኦዲት አተገባበር እና የደህንነት መንገዶች ጥልቅ ዕውቀት፤ ➢ ጥልቀት ያለው እና ተግባራዊ ማድረግ የሚችል የደህንነት መቆጣጠሪያ መንገዶች ዕውቀት፤	➢ የሰው ኃይል የመረጃ ደህንነት ንቃተ ህሊና ደረጃን መመዘን፤ ➢ ለኢላማው በሚሆን መልኩ የሚታወቁ የሰርጎ ገብ መፈጸሚያዎችን የማበጀት፤ ➢ በወጣው የደህንነት መስፈርት እና የስጋት ሞዴል መሰረት በራስ የሶርስ ኮድ ኦዲት የማድረግ፤ ➢ የተገኙ ክፍተቶችን ከኢላማው ፍላጎት እና ከተቋሙ አንጻር ተጨባጭ ምክረ	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ዲግሪ/ ሁለተኛ ዲግሪ፤	➢ የመጀመሪያ ዲግሪ ከ4 እስከ 5 ዓመት ወይም ➢ ሁለተኛ ዲግሪ 2 እስከ 3 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Ethical Hacking ወይም ➢ Source code audit (ቢኖር ይመረጣል)፤

ይተገብራል (manual source code audit)፤ ➢ ላገኛቸው ክፍተቶች ምክረ ሃሳብ ያቀርባል፤ ➢ የተሰጡ ምክረ ሃሳቦች ከአሁናዊ የደህንነት መጠበቂያ ዘዴዎች አንጻር በመተንተን ያስቀምጣል፤ ➢ ከበታቹ ለሚገኙ ባለሞያዎች ስልጠናዎችን ይሰጣል፤ ➢ የተገኙ ክፍተቶችን ሪፖርት ያደርጋል፤ ➢ ለተገኙ ክፍተቶች የስጋት ደረጃ ያስቀምጣል፤		ሃሳቦችን የማስቀመጥ፤			
የመወዳደሪያ አቅሞች	**ማብራሪያ**				
➢ መረጃ ማሰባሰብ፤	➢ የሳይበር ደህንነት ኦዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤				
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤				
➢ የሥራ ክባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች ከተቋሙ ራዕይ፣ ተልዕኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፍላጎቶች ጋር ያላቸውን ተጣጣሚነት የመገንዘብ ብቃት፤				

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት አዲት እና ግምገማ ባለሙያ

ደረጃ: V

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ➢ በተቀመጠው የስራ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ የሐሰት አሉታዊ (false negative) ወይም በራስ ሰር መተግበሪያዎች የማይለዩ ክፍተቶችን ይለያል፤ ➢ በራስ ክፍተቶችን ይለያል፤ የሲስተም አወቃቀር ይገመግማል (manual vulnerability assessment and configuration review)፤	➢ ሲስተም ሰኪዩሪቲ ዕውቀት፤ ➢ የአሰራር ሂደቶችን የመገንዘብ እና እንደ አስፈላጊነቱ የመምረጥ እና የመጠቀም እውቀት፤ ➢ የመመዘኛ እውቀት እና ዘዴዎችን የመምረጥ እና የመተግበር እውቀት፤ ➢ የውስጥ መመሪያን የመረዳት እና የመመሪያ አተገባበር የመመዘን እውቀት፤ ➢ የኔትዎርክ ንድፍ እና ተያያዝው የሚመጡ ክፍተቶች ዕውቀት፤ ➢ ፕሮጀክት አመራር እና አስተዳደር	➢ ችግሮችን በጥንቃቄ የመመርመር እና መፍትሄዎችን የመለየት፤ ➢ በራስ ክፍተቶችን የመለየት ዕውቀት፤ ➢ ሐሰት እና አሉታዊ ክፍተቶችን የመለየት፤ ➢ በራስ ክፍተቶችን የመለየት እና የሲስተም አወቃቀር የመገምገም (manual vulnerability assessment and configuration review)፤ ➢ የአሰራር ሂደቶችን እና የመመዘኛ ዝርዝሮችን	በኢንፎርሜሽን ሳይንስ፣ኮምፒውተር ሳይንስ፣ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ድግሪ ወይም ሁለተኛ ድግሪ፤	➢ የመጀመሪያ ዲግሪ ከ5 እስከ 6 ዓመት ወይም ➢ ሁለተኛ ዲግሪ 3 እስከ 4 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ System and Network Security ወይም ➢ Security system and network design ቢኖር ይመረጣል፤

➢ የአሰራር ሂደቶችን፣ የመመዘኛ ዝርዝሮችን እና ዘዴዎችን ይመርጣል፤ ➢ የውስጥ መመሪያዎች አተገባበር እና አከባበር ይገመግማል፤ ➢ የኔትዎርክ እና አፕሊኬሽን ንድፍ (design) ደህንነት ደረጃ ይገመግማል፤ ➢ በተቋሙ የሚካሄዱ ኦዲቶችን በተቀመጠው እቅድ መሰረት ያስጀምራል፣ ያስፈጽማል፤ ➢ ለተገኙ ክፍተቶች እና ከሱ በታች ባሉ ደረጃዎች ያስቀመጡትን ክፍተት ከተቋሙ አሁናዊ ሁኔታ ጋር ተልዕኮ እና አቅም አንጻር ያደራጃል፤ ➢ ለተገኙ ክፍተቶች የተቋሙን አሁናዊ ሁኔታ፣ አቅም እና ስርዓት ባገናዘበ አካሄድ የክፍተቱን የስጋት ደረጃ ያስቀምጣል፤ ➢ ከታች ለሚገኙ ባለሙያዎች ስልጠናዎችን ይቀርጻል፣ ይሰጣል፤	ዕውቀት፤ ➢ የተቋምን ተልዕኮ የመረዳት እና ተያያዥ የደህንነት ክፍተቶች ትንታኔ እውቀት፤ ➢ የስጋት ደረጃ አመዳደብ እውቀት፤	ከኢላማው አንጻር የመምረጥ እና የመተግበር፤ ➢ የኔትዎርክ እና አፕሊኬሽን ንድፍ (design) ከደህንነት አንጻር በመተንተን ክፍተቶችን የመለየት፤ ➢ ምክረ ሃሳቦችን የማቅረብ እና ከተቋሙ አቅም አንጻር የመመዘን፤ ➢ መደረግ ያለባቸው ቅደመ ዝግጅቶችን በማድረግ በተቋሙ ውስጥ የሚካሄዱ ኦዲቶችን የማስጀመር እና የማስፈጸም ክህሎት፤ ➢ ስልጠና የመቅረጽ እና ስልጠና የመስጠት፤			

➢ የምዘና ሪፖርቶችን (Technical Report) አጠናቅሮ ያቀርባል፤					

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ መረጃን ማሰባሰብ፤	➢ የሳይበር ደህንነት ኦዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤
➢ ተጋላጭነት ግምገማ፤	➢ የተቋሙን ቁልፍ የመረጃ ስርዓቶች፣ መረጃዎች እና መሰረተ-ልማቶች ጥቃት እንዳይደርስባቸው የኢላማውን ደካማ ጎኖች ወይም ክፍተቶችን በራስ ሰር (automated) ቱሎችን በመጠቀም የመለየት፣ የመገምገም እና ሪፖርት የማድረግ፤
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤
➢ የሥራ ከባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች ከተቋሙ ራዕይ፣ ተልዕኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፍላጎቶች ጋር ያላቸውን ተጣጣሚነት የመገንዘብ ብቃት፤

የሥራ መደብ መጠሪያ፡ የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ

ደረጃ፡ VI

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ ከሱ በታች ባሉ ደረጃዎች የሚወጡ እቅዶችን ከተቋሙ እና ከክፍሉ እቅድ አንጻር ይገመግማል፣ ያረጋግጣል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ➢ በተቋሙ እቅድ መሰረት የራሱ እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ በተቋሙ አጠቃላይ የአሰራር ሂደት ላይ	➢ የተቋሙን አላማ እና የአሰራር ሂደት በጥልቀት የመረዳት እና የመተንተን እውቀት፤ ➢ በአሰራር ደረጃ ያሉ የደህንነት ክፍተቶችን የመለየት እና የመፍትሄ ምክረ ሃሳቦች አቀራረብ እውቀት፤ ➢ የደህንነት መመሪያዎችን መረዳት እና በማበልጸግ ሂደት ውስጥ ተደራሽ መደረግ ያለባቸውን ነጥቦች እውቀት እና በዚያ መሰረት የመገምገም እውቀት፤ ➢ የስጋት ሞዴል የማበልጸግ፣ የመረዳት እና የመገምገም	➢ የሙከራ ጉዳዮችን (test case) የማበልጸግ፤ ➢ የስጋት ሞዴሎችን የመገምገም፤ ➢ መተዳደሪያ ደንቦችን ከደህንነት አንጻር የመገምገም፤ ➢ በተቋም ደረጃ ችግሮችን በጥንቃቄ የመመርመር እና መፍትሄዎችን የመለየት፤ ➢ የኦዲት ስራዎችን የመምራት እና	➢ በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ዲግሪ ወይም ሁለተኛ ዲግሪ	➢ የመጀመሪያ ዲግሪ ከ6 እስከ 7 ዓመት ወይም ➢ ሁለተኛ ዲግሪ 4 እስከ 5 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Threat modeling ወይም ➢ Policy development ወይም ➢ Information security analyst ቢኖር ይመረጣል፤

የደህንነት ምዘና ያካሂዳል፤ ➢ የሙከራ ጉዳዮችን (test case) ያበለጽጋል፤ ➢ የውስጥ ኢቴክ እና ተያያዥ መተዳደሪያ ደንቦችን (Internal Policies) ከደህንነት አንጻር ይገመግማል፣ ይመዘናል፤ ➢ ለኢላማዎች የስጋት ሞዴል (Threat Model) ይገመግማል፣ ይመዘናል፤ ➢ በተቋሙ ውስጥ የሚሰሩ የኦዲት ስራዎችን ይከታተላል፣ ይቆጣጠራል ፣ሪፖርት ያደራጃል፤ ➢ ከታች ለሚገኙ ባለሙያዎች ስልጠናዎችን ይቀርጻል፣ ይሰጣል፤ ➢ ተቋሙ ባስቀመጠው እቅድ ወይም በየ 6 ወሩ የቴክኒካል ሪፖርት ለበላይ አመራር ያቀርባል፤	እውቀት ➢ የአመራር እውቀት፤	የመቆጣጠር፤ ➢ የተሰሩ ስራዎችን የማቅረብ እና ከባለድርሻ አካላት ጋር ግንኙነትን በመፍጠር የመምራት፤			
የመወዳደሪያ አቅሞች	**ማብራሪያ (Description)**				
➢ መረጃን የማሰባሰብ አቅም፤	➢ የሳይበር ደህንነት ኦዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤				

➢ ተጋላጭነት ግምገማ፤	➢ የተቋሙን ቁልፍ የመረጃ ስርዓቶች፣ መረጃዎች እና መሰረተ-ልማቶች ጥቃት እንዳይደርስባቸው የኢላማውን ደካማ ጎኖች ወይም ክፍተቶችን በራስ ሰር (automated) ቱሎችን በመጠቀም የመለየት፣ የመገምገም እና ሪፖርት የማድርግ፤
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤
➢ የሥራ ክባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች ከተቋሙ ራዕይ፣ ተልዕኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፍላጎቶች ጋር ያላቸውን ተጣጣሚነት የመገንዘብ ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ

ደረጃ: VII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬቶች
➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ➢ በተቀመጠው የክፍሉ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ የምዘና መስፈርቶችን (Checklists)፣ የአሰራር ሂደቶችን (Procedures) እና ዘዴዎችን (Methodologies) ለተቋሙ እና ለኢላማዎች በሚሆን መልኩ ያበጃል	➢ የምዘና መስፈርቶች (Checklists)፣ የአሰራር ሂደቶች (Procedures) እና ዘዴዎች (Methodologies) እውቀት፤ ➢ በሃገር አቀፍ ደረጃ የወጡ መመሪያዎች እና ደረጃዎችን በጥልቀት ማወቅ፤ ➢ ተቋሙ የሚከተላቸውን እና የሚገደድባቸውን ደረጃዎች ማወቅ እና መረዳት፤ ➢ በክፍተቶች ምክንያት የሚመጡ ተጽዕኖዎችን ማወቅ እና ከተቋም አንጻር የማስተሳሰር እውቀት፤	➢ የምዘና መስፈርቶችን (Checklists)፣ የአሰራር ሂደቶችን (Procedures) እና ዘዴዎች (Methodologies)፤ ➢ ለተቋሙ እና ለኢላማው በሚሆን መልኩ ማበጀት (Customization) እና ማላመድ፤ ➢ ሃገር አቀፍ መመሪያዎችን በመጠቀም የአከባበር አዲት ማከናወን፤	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ፤የመጀመሪያ ዲግሪ ወይም ሁለተኛ ዲግሪ	የመጀመሪያ ዲግሪ ከ7 እስከ 8 ዓመት ወይም ሁለተኛ ዲግሪ 5 እስከ 6 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Certified Information Security Auditor ቢኖር ይመረጣል፤

(Customization) እና ያላምዳል፤ ➢ በሃገር አቀፍ ደረጃ የወጡ መመሪዎችን እና ስታንዳርዶችን በመጠቀም አተገባበር እና አከባበርን ይገመግማል፤ ➢ ዓለም ዓቀፍ ደረጃዎችን በመጠቀም አተገባበር እና አከባበርን ይገመግማል፤ ➢ በተቋሙ የሚደረጉ የኦዲት ክንዋኔዎችን የአተገባበር እቅድ ያወጣል፤ ➢ ምክረ ሃሳቦችን ከተቋሙ አሁናዊ ሁኔታ ጋር በማዛመድ የአተገባበር ቅድመ ተከተል ምክረ ሃሳብ ያቀርባል፤ ➢ ከታች ለሚገኙ ባለሞያዎች ስልጠናዎችን ይቀርጻል፣ ይሰጣል፤ ➢ ተጽዕኖዎችን ከተቋም አንጻር ከክፍተቶች ጋር አሰተሳስሮ ያቀርባል፤		➢ እቅድ ማውጣት እና አተገባበሩ መከታተል እና መምራት፤ ➢ በተቋም ደረጃ ለተገኙ የክፍተቶችን ተጽዕኖ መጠን በመተንተን ማቅረብ፤			
የመወዳደሪያ አቅሞች	**ማብራሪያ**				
➢ መረጃን ማሰባሰብ፤	➢ የሳይበር ደህንነት ኦዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደረጀት፤				
➢ ተጋላጭነት ግምገማ፤	➢ የተቋሙን ቁልፍ የመረጃ ስርዓቶች፣ መረጃዎች እና መሰረተ-ልማቶች ጥቃት እንዳይደርስባቸው የኢላማውን ደካማ				

	ሳኖች ወይም ክፍተቶችን በራስ ሰር (automated) ቱሎችን በመጠቀም የመለየት፣ የመገምገም እና ሪፖርት የማድርግ
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤
➢ የሥራ አባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች ከተቋሙ ራዕይ፣ ተልዕኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፍላጎቶች ጋር ያላቸውን ተጣጣሚነት የመገንዘብ ብቃት፤

የሥራ መደብ መጠሪያ: የሳይበር ደህንነት ኦዲት እና ግምገማ ባለሙያ
ደረጃ: VIII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ በክፍሉ የሚሰሩ እና የታቀዱ ስራዎችን በመተንተን በተዋረድ ወደታች ያወርዳል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት ይቆጣጠራል፤ ➢ የምዘና መስፈርቶችን (Checklists)፣ የአሰራር ሂደቶችን (Procedures) እና ዘዴዎችን (Methodologies) ያበለጽጋል፤ ➢ አለም አቀፍ ስታንዳርዶችን በመጠቀም	➢ የምዘና መስፈርቶችን (Checklists)፣ የአሰራር ሂደቶችን (Procedures) እና ዘዴዎችን (Methodologies) የማወቅ እና የማበልጸግ እውቀት፤ ➢ የመምራት እና ስልታዊ እቅዶችን የማውጣት እውቀት፤ ➢ ስልጠና የመስጠት እና የመቅረጽ እውቀት፤ ➢ በተቋም ደረጃ የአሰራር ሂደቶችን መገንዘብ እና በግምገማ ሂደት ውስጥ ለሚገኙ ክፍተቶች	➢ ስልታዊ እቅድ መቅረጽ መቻል፤ ➢ ከባለድርሻ አካላት ጋር ግንኙነት የማድረግ፤ ➢ የምዘና መስፈርቶችን (Checklists)፣ የአሰራር ሂደቶችን (Procedures) እና ዘዴዎችን (Methodologies) የማበልጸግ፤ ➢ የተቋሙን አጠቃላይ የአሰራር ሂደት	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ድግሪ ወይም ሁለተኛ ድግሪ	የመጀመሪያ ዲግሪ ከ8 እስከ 9 ዓመት ወይም ሁለተኛ ዲግሪ 6 እስከ 7 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Lead auditor

አተገባበር እና አከባበርን ይገመግማል፤ ➢ ተጨባጭ እና የተቋሙን ሁኔታ ባገናዘበ መልኩ ምክረ ሃሳብ ያቀርባል፤ ➢ የተቋሙን የኦዲት ስራ እና አተገባበር ስልታዊ (strategic) እቅድ ያዘጋጃል፣ ይመራል፤ ➢ የተቋሙን አጠቃላይ የአሰራር ሂደት ያጠናል፣ ምርጥ ተሞክሮዎችን እና አዳዲስ አካሄዶችን እና ምክረሃሳቦችን ያቀርባል፣ ይተገብራል፤ ➢ ከታች ለሚገኙ ባለሞያዎች ስልጠናዎችን ይቀርጻል፣ ይሰጣል፤ ➢ የተቋሙን እቅድ ወይም አመታዊ ሪፖርት ያቀርባል፤ ➢ ከሌሎች ክፍሎች እና ተቋማት ጋር እንደ አስፈላጊነቱ ግንኙነት ያደርጋል፤	ስልታዊ ምክረ ሃሳብ የማቅረብ እውቀት፤ ➢ በአለም አቀፍ ደረጃ የወጡ ስታንደርዶች ዕውቀት እና ግንዛቤ፤	በማጥናት፣ ምርጥ ተሞክሮዎችን እና አዳዲስ አካሄዶችን እና ምክረሃሳቦችን የማቅረብ እና የመተግበር፤ ➢ አለም አቀፍ ስታንዳርዶችን በመጠቀም የአተገባበር እና የአከባበር ግምገማ ክህሎት፤ ➢ አጠቃላይ የኦዲት ስራን የመምራት፤			
የመወዳደሪያ አቅሞች	**ማብራሪያ**				

➢ መረጃን ማሰባሰብ፤	➢ የሳይበር ደህንነት ኦዲት እና ግምገማው የሚከናወንበት ኢላማ በጥልቀት በመረዳት፤ ለግምገማው ዓላማ መሳካት የሚያግዙና በቀጣይ ለሚሰሩ ስራዎች መሰረት የሚሆኑ በአጠቃላይ የግምገማውን ሙሉ ምስል ማሳየት በሚያስችል መልኩ መረጃዎችን መሰብሰብ እና ማደራጀት፤
➢ ተጋላጭነት ግምገማ፤	➢ የተቋሙን ቁልፍ የመረጃ ስርዓቶች፣ መረጃዎች እና መሰረተ-ልማቶች ጥቃት እንዳይደርስባቸው የኢላማውን ደካማ ጎኖች ወይም ክፍተቶችን በራስ ሰር (automated) ቱሎችን በመጠቀም የመለየት፣ የመገምገም እና ሪፖርት የማድርግ
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት፤	➢ በሳይበር ደህንነት ላይ በሚደረጉ የኦዲትና ግምገማ ሂደቶች ውስጥ ተሳታፊ ከሚሆኑ ከሚመለከታቸው አካላት ጋር በመገናኘት በትብብር የመስራት እና የመግባባት አቅም፤
➢ የሥራ ክባቢ የመገንዘብ ብቃት፤	➢ የሳይበር ደህንነት አስተዳደር ስራዎች ከተቋሙ ራዕይ፣ ተልዕኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፣ ፍላጎቶች፣ ጋር ያላቸውን ተጣጣሚነት የመገንዘብ ብቃት፤

3.5. **የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ቡድን (ክፍል)**

የሥራ መደብ :- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ

ደረጃ፡ I

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ በተሰጠው የስራ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ በሲስተም ደረጃ የሚገኙ የተለያዩ እሴቶችን ከፋፍሎ የሳይበር ጥቃት ዲቴክሽን/ሞኒተሪንግ/ ማከናወን፤ ➢ በሲስተም ደረጃ የሳይበር ጥቃት አርቲፋክት	➢ ዌብላንጉች (ፒ.ኤች.ፒ፤ ኤስ.ፒ፤ ኤች.ቲ.ኤም.ኤል፣ወዘተ) ➢ ኔትወርኪንግ ➢ Internet and cloud ➢ Internet programming ➢ Operating system ➢ መሰረታዊ የሳይበር ጥቃት እውቀት፤ ➢ Network and host	➢ በአንድ ሲስተም (Hosts) ደረጃ የተገጠሙ የዲቴክሽን የፐሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በሙሉ ብቃት መጠቀም መቻል፣ስለተመደበበት ሲስተም አሰራር (day-to-day activities, input and outputs, etc) በጥልቀት ማወቅ እና ከሳይበር ጥቃት አንፃር መረዳት፤ ➢ በተቋም ደረጃ የተገጠሙ የዲቴክሽን የፐሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በመጠቀም የተመደበበት ሲስተም ላይ የሚደርሱ true positive ጥቃቶችን መለየትና	በኢንፎርሜሽን ሳይንስ፣ኮምፒውተር ሳይንስ፣ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ትመስክ የመጀመሪያ ዲግሪ፤	የመጀመሪያ ዲግሪ 0 ዓመት፤	

መሰብሰብ፤ ➢ በሲስተም ደረጃ የጥቃቶች ትንተና በመስራት መረጃ ማቅረብ፤ ➢ አስተያየት እና ሪፖርት ማዘጋጀት፤ ➢ በሲስተም ደረጃ ለጥቃቶች ተገቢውን ምላሽ መስጠት፤ ➢ በሲስተም ደረጃ የvulnerability assessment ማካሄድና ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ በሲስተም ደረጃ False positive alerts ለይቶ ማቅረብ፤	security detection, prevention and monitoring devices ➢ ኢንትሩሽን ዲቴክሽን ➢ knowledge of log management and correlation፤	የመጀመሪያ ደረጃ analysis መስራት (የስራ መመሪያዎች /Working Manual/ መርሆች, procedures, policies መሰረት በማድረግ)፤ ➢ የተፈጠረውን ክስተት ምልክት ለሚያደርጉ ማንቂያ ደውሎች አዲስ የክስተት (incident)ትኬቶችን ይፈጥራል፤ ➢ በተመደበበት ሲስተም ደረጃ ሎግ፤ኢቨንት፤ ትራፊክ፤ወዘተ ላይ ዳታ/አርቲፋክት መሰብሰብ፤ ➢ በተመደበበት ሲስተም ደረጃ እንግዳ የሆነ እንቅስቃሴ በማየት አርቲፋክት ለይቶ መሰብሰብ፤ ➢ በተመደበበት ሲስተም ደረጃ ሪሶርስ (ራም፤ ሲፒዩ፤ባንድዊድዝ፤ወዘተ) አናሊሲስ፤ ➢ በሲስተም ደረጃ በዲቴክሽን true positive ተብለው የተለዩ ጥቃቶችን የተሰበሰቡትን ዳታ/አርቲፋክት በመጠቀም ጠለቅ ያለ አናሊሲስ በመስራት የተቋመን የሪፖርት መስፈርት ተከትሎ ሪፖርት እና ሪኮመንዴሽን ማምረት፤ ➢ በሲስተም ደረጃ ለደረሱ ጥቃቶች ተገቢውን የምላሽ መስጠት ማከናወን፤ ➢ በሲስተም ደረጃ የሚገኙ የተለያዩ እሴቶችን ለሞኒተሪንግ በሚያመች መልኩ መከፋፈል እና ሊደርሱ የሚችሉባቸውን የሳይበር ጥቃቶች መዘርዘር (scenarios)፤ ➢ ከእሴቶቹ መገኘት በሚችሉ ዳታ መሰረት ለጥቃቶቹ ተገቢውን የዲቴክሽን ሩል			

		ማዘጋጀትና ለደረጃ 3 ሰራተኞች ማቅረብ፤ ➢ በተቋሙ ዉስጥ የሚገኙ የሳይበር ደህንነት ክፍተቶች መመዘኛ መሳሪያዎች በመጠቀም በሲስተም ደረጃ በተሰጠው የጊዜ ሰሌዳ እና ወሰን መሰረት vulnerability assessment ማካሄድ፤ ➢ በሲስተምደረጃ vulnerability assessment ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ በሲስተም ደረጃ False positive ተብለው የተለዩ alerts ለደረጃ 3 ሰራተኞች ማቅረብ (if the rule is defective or generating false positive)፤ ➢ ትንተና የተሰራባቸውን ጥቃቶች በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ፤			
የመወዳደሪያ አቅሞች		**ማብራሪያ**			
➢ ጥቃቶችን ዲቴክት ማድረግ፤		➢ የሳይበር ጥቃቶችን መለያ መንገዶችን በማወቅ ጥቃቶችን ዲቴክት ማድረግ፤			
➢ False positive እና true positive የሳይበር ጥቃቶችን መለየት፤		➢ በተመደበበት ሲስተም ላይ የሚታዩ ትክክለኛ ጥቃቶችን በመለየት ሞኒተር ማድረግ፤			
➢ አርቲፋክት መሰብሰብ፤		➢ በሲስተም ደረጃ ጥቃቶች ላይ ጥልቅ አናሊሲስ ሊያሰሩ የሚችሉ የተለያዩ አርቲፋክቶችን የሚቀመጡበትን ቦታዎች ማወቅ እና መሰብሰብ፤			
➢ አናሊሲስ/ትንተና፤		➢ በሲስተም ደረጃ የተሰበሰቡ አርቲፋክቶችን ከተለያዩ የጥቃቱ ሁኔታዎች፣ የሲስተሙ አቋም፣ ወዘተ ጋር በማገናኘትና በማገናዘብ ስለጥቃቱ የተለያዩ ዝርዝሮችን (ምን አይነት ጥቃት ነው፣ አላማው ምንድነው፣ ምን ጉዳት አስከተለ፣ የተጠቀማቸው ዘዴዎች፣ ጥቃቱን መከላከልና ዲቴክት ማድረግ የሚያስችሉ ድክመቶች፣ መለያዎች፣ መፍትሄዎች፣ ወዘተ) ማውጣት፣ የተለያዩ ጥቃቶችን			

	ማስተሳሰር፤
➢ ምላሽ መስጠት፤	➢ በሲስተም ደረጃ ጥቃት የደረሰባቸውን ወይም ሊደርስባቸው የሚችሉ software እና/ወይም hardware ጉዳቱን በሚመልስ እና ጥቃቱ ተመልሶ በማያጠቃው መልኩ ምላሽ መስጠት፤

የሥራ መደብ ፡- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ

ደረጃ፡ II

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ በደረጃ 1 የተጠቀሱትን በብቃት ማከናወን መቻል፤ ➢ በደረጃ 1 ባሉ ባለሞያዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ በደረጃ 1 የተሰሩ ስራዎችን ጥራት መቆጣጠር እና ማረጋገጥ፤	➢ ዌብላንጉች (ፒኤችፒ፤ኤሴፒ፤ ኤች.ቲ.ኤም.ኤል.፣ ወዘተ) ➢ ኔትወርኪንግ ➢ Internet and cloud ➢ Internet programming ➢ ኔትወርክ ሴክዩሪቲ ➢ Operating system ➢ መሰረታዊ የሳይበር	➢ በሲስተም ደረጃ የተሰሩ ስራዎችን ማረጋገጥ፤ ➢ ከሁለት እና ከዛበላይ የሆኑ ሲስተሞች (Hosts) ደረጃ የተገጠሙ የዲቴክሽን የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በሙሉ ብቃት መጠቀም መቻል፣ ስለተመደበበት ሲስተሞች አሰራር (day-to-day activities, input and outputs, etc) በጥልቀት ማወቅ እና ከሳይበር ጥቃት አንፃር መረዳት፤ ➢ በተቋም ደረጃ የተገጠሙ የዲቴክሽን የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በመጠቀም የተመደበበት ሁለት እና ከዛበላይ የሆኑ ሲስተሞች ላይ የሚደርሱ	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ትመስክ የመጀመሪያ	የመጀመሪያ ዲግሪ 1 እስከ 2 ዓመት አግባብነት ያለው የሥራ ልምድ ሁለተኛ ዲግሪ 0 ዓመት፤	

➢ በተሰጠው የስራ እቅድ መሰረት የራሱ እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ የሚገኙ የተለያዩ እሴቶችን ከፋፍሎ የሳይበር ጥቃት ዲቴክሽን/ሞኒተሪንግ ማከናወን፤ ➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ የሳይበር ጥቃት አርቲፋክት መሰብሰብ፤ ➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ የጥቃቶች ትንታና በመስራት መረጃ ማቅረብ፤ ➢ አስተያየት እና ሪፖርት ማዘጋጀት፤ ➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ ለጥቃቶች ተገቢውን ምላሽ መስጠት፤	ጥቃት እውቀት፤ ➢ Network security monitoring፤ ➢ Network and host security detection, prevention and monitoring devices ➢ ኢንትሩዥን ዲቴክሽን፤ ➢ Threat hunting and artifact collection ➢ ኢንትሩዥን ትንተና፤ ➢ knowledge of log management and correlation ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣እቅድ የማውጣት እና የመምራት እውቀት፤	true positive ጥቃቶችን መለየትና የመጀመሪያ ደረጃ analysis መስራት (የስራ መመሪያዎች /Working Manual/ መርሆች፣ procedures, policies መሰረት በማድረግ)፤ ➢ የተፈጠረውን ክስተት ምልክት ለሚያደርጉ ማንቂያ ደውሎች አዲስ የክስተት (incident) ትኬቶችን ይፈጥራል፤ ➢ በተመደበበት ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ ሎግ፣ ኢቨንት፣ ትራፊክ፣ ወዘተ ላይዳታ/ አርቲፋክት መሰብሰብ፤ ➢ በተመደበበት ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ እንግዳ የሆነ እንቅስቃሴ በማየት አርቲፋክት ለይቶ መሰብሰብ፤ ➢ በተመደበበት ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ ሪሶርስ (ራም፣ሲፒዩ፣ባንድዊድዝ፣ወዘተ) አናሊሲስ፣ ➢ ከሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ በዲቴክሽን true positive ተብለው የተለዩ ጥቃቶችን የተሰበሰቡትን ዳታ/አርቲፋክት በመጠቀም ጠለቅ ያለአናሊሲስ በመስራት የተቋሙን የሪፖርት መስፈርት ተከትሎ ሪፖርት እና ሪኮመንዴሽን ማምረት፤ ➢ በሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ ለደረሱ ጥቃቶች ተገቢውን ምላሽ የመስጠት፤ ➢ ከሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ	ወይም ሁለተኛ ዲግሪ፤		

➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ የ vulnerability assessment ማካሄድና ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ False positive alerts ለይቶ ማቅረብ፤		የሚገኙ የተለያዩ እሴቶችን ለሞኒተሪንግ በሚያመች መልኩ መከፋፈል እና ሊደርሱ የሚችሉባቸውን የሳይበር ጥቃቶች መዘርዘር (scenarios)፡፡ከእሴቶቹ መገኘት በሚችሉ ዳታ መሰረት ለጥቃቶቹ ተገቢውን የዲቴክሽን ሩል ማዘጋጀትና ለደረጃ 3 ሰራተኞች ማቅረብ፤ ➢ በተቋሙ ውስጥ የሚገኙ የሳይበር ደህንነት ክፍተቶች መመዘኛ መሳሪያዎች በመጠቀም ከሁለት እና ከዛበላይ የሆኑ ሲስተሞች ደረጃ በተሰጠው የጊዜ ሰሌዳ እና ወሰን መሰረት vulnerability assessment ማካሄድ፤ ➢ ከሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ በ vulnerability assessment ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ ከሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ False positive ተብለው ለተለዩ alerts ለደረጃ 3 ሰራተኞች ማቅረብ (if the rule is defective or generating false positive)፤ ➢ አናሊሲስ የተሰራባቸውን ጥቃቶች በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ፤			
የመወዳደሪያ አቅሞች		**ማብራሪያ**			
➢ ጥቃቶችን ዲቴክት ማድረግ፤		➢ የሳይበር ጥቃቶች መለያ መንገዶችን በማወቅ ጥቃቶችን ዲቴክት ማድረግ፤			
➢ False positive እና true positive የሳይበር ጥቃቶችን መለየት፤		➢ በተመደበበት ሁለት እና ከዛ በላይ የሆኑ ሲስተሞች ላይ የሚታዩ ትክክለኛ ጥቃቶችን በመለየት ሞኒተር ማድረግ፤			
➢ አርቲፋክት መሰብሰብ፤		➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ ጥቃቶች ላይ ጥልቅ አናሊሲስ ሊያሰሩ የሚችሉ የተለያዩ አርቲፋክቶችን የሚቀመጡበትን ቦታዎች ማወቅ እና መሰብሰብ፤			
➢ አናሊሲስ/ትንተና፤		➢ ሁለት እና ከዛ በላይ በሆኑ ሲስተሞች ደረጃ የተሰበሰቡ አርቲፋክቶችን ከተለያዩ የጥቃቱ ሁኔታዎች፣ የሲስተሞች አቋም፣ ወዘተ ጋር በማገናኘትና በማገናዘብ ስለ ጥቃቱ የተለያዩ ዝርዝሮችን (ምን አይነት			

	ጥቃት ነው፣ አላማው ምንድነው፣ ምን ጉዳት አስከተለ፣ የተጠቀማቸው ዘዴዎች፣ ጥቃቱን መከላከልና ዲቴክት ማድረግ የሚያስችሉ ድክመቶች፣ መለያዎች፣ መፍትሄዎች፣ ወዘተ) ማውጣት፣ የተለያዩ ጥቃቶችን ማስተሳሰር፤
➢ ምላሽ መስጠት፤	➢ ሁለት እና ከዚያ በላይ የሆኑ ሲስተሞች ደረጃ ጥቃት የደረሰባቸውን ወይም ሊደርስባቸው የሚችሉ software እና/ወይም hardware ጉዳቱን በሚመልስ እና ጥቃቱ ተመልሶ በማያጠቃው መልኩ ምላሽ መስጠት፤

የሥራ መደብ :- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ
ደረጃ: III

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ ከደረጃ 3 በታች የተጠቀሱትን ኃላፊነቶች በብቃት ማከናወን መቻል፤ ➢ ከደረጃው በታች የሚሰሩ ሰራዎችን ያቅዳል፣ይመራል፤ ያበቃል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት መቆጣጠር፣ ➢ ከደረጃው በታች ላሉ አባላት	➢ ቄብላንጉች (ፒኤችፒ፤ኤስፒ፤ ኤች.ቲኤም.ኤል፣ ወዘተ) ➢ ኔትወርኪንግ ➢ Internet and cloud ➢ Internet programming ➢ ኔትወርክ ሴክዩሪቲ ➢ Operating	➢ በሁለት እና ከዛ በላይ ያሉ ሲስተም ደረጃ የተሰሩ ስራዎችን ማረጋገጥ፤ ➢ በዲፖርትመንት/በቅርንጫፍ/ዲቪሻርን (Hosts) ደረጃ የተገጠሙ የዲቴክሽን የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በሙሉ ብቃት መጠቀም መቻል፣ ስለተመደበበት ሲስተሞች አሰራር (day-to-day activities, input and outputs, etc) በጥልቀት ማወቅ እና ከሳይበር ጥቃት አንፃር መረዳት፤ ➢ በተቋም ደረጃ የተገጠሙ የዲቴክሽን	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ፤	➢ የመጀመሪያ ዲግሪ 2 እስከ 3 ዓመት ➢ ሁለተኛ ዲግሪ 0 እስከ 1 ዓመት አግባብነት ያለው የሥራ	➢ Cyber security monitoring (training or certification ወይም ➢ CCNA (training or certifcation ወይም ➢ CCNA

ማሰልጠን እና ማብቃት፤ ➢ በዲፖርትመንት/ በቅርንጫፍ/ዲቪዥን ደረጃ የሚገኙ የተለያዩ እሴቶችን ከፋፍሎ የሳይበር ጥቃት ዲቴክሽን/ሞኒተሪንግ/ ማከናወን፤ ➢ በዲፖርትመንት/በቅርንጫፍ/ ዲቪዥን ደረጃ የሳይበር ጥቃት አርቲፋክት መሰብሰብ፤ ➢ በዲፖርትመንት/በቅርንጫፍ/ዲ ቪዥን ደረጃ የጥቃቶች አናሊሲስ በመስራት መረጃ ማቅረብ፤ ➢ አስተያየት እና ሪፖርት ማዘጋጀት፤ ➢ በዲፖርትመንት/በቅርንጫፍ/ዲ ቪዥን ደረጃ ለጥቃቶች ተገቢውን ምላሽ መስጠት፤ ➢ በአንድና ከዛ በላይ ሲስተሞች፣ በዲፖርትመንት/በቅርንጫፍ/ ዲቪዥን ደረጃ ላሉ ጥቃቶች ሩል እና/ወይም/ ስግኒቸር, IOC ማስተካከል እና አዳዲስ መጨመር፤	system ➢ አድቫንስድ የሳይበር ጥቃት እውቀት፤ ➢ Network security monitoring ➢ Network and host security detection, prevention and monitoring devices ➢ አድቫንስድ ኢንትሩዥን ዲቴክሽን ➢ Threat hunting and artifact collection ➢ አድቫንስድ ኢንሲደንት ሃንድሊንግ ➢ Data and system recovery ➢ knowledge of log management	የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በመጠቀም የተመደበበት በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ ያሉ ሲስተሞች ላይ የሚደርሱ true positive ጥቃቶችን መለየትና የመጀመሪያ ደረጃ analysis መስራት (የስራ መመሪያዎች /Working Manual/ መርሆች, procedures, policies መሰረት በማድረግ)፤ ➢ የተፈጠረውን ክስተት ምልክት ለሚያደርጉ ማንቂያ ደውሎች አዲስ የክስተት (incident)ትኬቶችን ይፈጥራል፤ ➢ በተመደበበት በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ ሎግ፤ኢቭንት፤ትራፊክ፤ወዘተ ላይ ዳታ/አርቲፋክት መሰብሰብ፤ ➢ በተመደበበት በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ እንግዳ የሆነ እንቅስቃሴ በማየት አርቲፋክት ለይቶ መሰብሰብ፤ ➢ በተመደበበት በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ ሪሶርስ (ራም፤ሲፒዩ፤ባንድዊድዝ፤ወዘተ) አናሊሲስ ➢ በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ በዲቴክሽን true positive ተብለው የተለዩ		ልምድ፤	security ወይም ➢ Continuous monitoring certification ወይም ➢ Security essentials ወይም ➢ Certified SOC analyst ወይም ➢ Certified incident handler ወይም ➢ Cyber threat hunting ወይም ➢ Certified intrusion analyst ቢኖር ይመረጣል፤

➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ የ vulnerability assessment ማካሄድና ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ በአንድና ከዚያ በላይ ሲስተሞች፣ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ ለFalse positive alerts የዲቴክሽን ሩል ማስተካከል፤ ➢ የሞኒተሪንግ ሥራ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን እሴቶች ደረጃ ማስፋት፤	and correlation ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣ እቅድ የማውጣት እና የመምራት እውቀት፤	ጥቃቶችን የተሰበሰቡትን ዳታ/አርቲፋክት በመጠቀም ጠለቅ ያለ አናሊሲስ በመስራት የተቋሙን የሪፖርት መስፈርት ተከትሎ ሪፖርት እና አስተያየት ማቅረብ፤ ➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ ለደረሱ ጥቃቶች ተገቢውን የምላሽ መስጠት ማከናወን ➢ በአንድና ከዚያ በላይ ሲስተሞች፣ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ የጥቃት አናሊሲስ በሚገኙ ዉጤቶች መሰረት የዲቴክሽን፣ፕሪቬንሽን እና ሞኒተሪንግ ሲስተሞችን ሩል እና/ወይም ስግኒቸር, IOC ማስተካከል እና አዳዲስ መጨመር፤ ➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ የሚገኙ የተለያዩ እሴቶችን ለሞኒተሪንግ በሚያመች መልኩ መከፋፈል እና ሊደርሱ የሚችሉባቸውን የሳይበር ጥቃቶች መዘርዘር (scenarios)። ከእሴቶቹ መገኘት በሚችሉ ዳታ መሰረት ለጥቃቶቹ ተገቢውን የዲቴክሽን ሩል መስራት፤ ➢ በተቋሙ ዉስጥ የሚገኙ የሳይበር ደህንነት ክፍተቶች መመዘኛ መሳሪያዎች በመጠቀም በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ በተሰጠው የጊዜ ሰሌዳ እና ወሰን መሰረት vulnerability assessment ማካሄድ፤			

		➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ በ vulnerability assessment ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ በአንድና ከዚያ በላይ ሲስተሞች፣ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ False positive ተብለው ለተለዩ alerts የዲቴክሽን ሩል ማስተካከል (if the rule is defective or generating false positive) ➢ በሲስተሞች በዲፓርትመንት /በቅርንጫፍ/ ዲቪዥን/ ደረጃ ሞኒተር የሚደረጉ አዳዲስና ያልገቡ እሴቶችን ወደ ሞኒተሪንግ ሲስተምስ ማቀላቀል፤ ➢ በየጊዜው የሚያጋጥሙ ተግዳሮቶች የተፈቱበትን እውቀት መሰነድ (አናሊሲስ የተሰራባቸውን ጥቃቶች በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ)፣ በተጨማሪም የተስተካከሉ ወይም አዳዲስ የተጨመሩ ሩሎችን ከነዝርዝራቸው በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ፤			

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ ጥቃቶችን ዲቴክት ማድረግ፤	➢ የሳይበር ጥቃቶችን መለያ መንገዶችን በማወቅ ጥቃቶችን ዲቴክት ማድረግ፤
➢ False positive እና true positive የሳይበር ጥቃቶችን መለየት፤	➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን (Hosts) ደረጃ የሚታዩ ትክክለኛ ጥቃቶችን በመለየት ሞኒተር ማድረግ፤
➢ አርቲፋክት መሰብሰብ፤	➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን (Hosts) ደረጃ ጥቃቶች ላይ ጥልቅ አናሊሲስ ሊያሰሩ የሚችሉ የተለያዩ አርቲፋክቶችን የሚቀመጡበትን ቦታዎች ማወቅ እና መሰብሰብ፤
➢ አናሊሲስ/ትንተና፤	➢ በዲፓርትመንት/በቅርንጫፍ/ዲቪዥን (Hosts) ደረጃ የተሰበሰቡ አርቲፋክቶችን ከተለያዩ የጥቃቱ ሁኔታዎች፣ የሲስተሞች አቋም፣ ወዘተ ጋር በማገናኘትና በማገናዘብ ስለ ጥቃቱ የተለያዩ ዝርዝሮችን

	(ምን አይነት ጥቃት ነው፣ አላማው ምንድነው፣ ምን ጉዳት አስከተለ፣ የተጠቀማቸው ዘዴዎች፣ ጥቃቱን መከላከልና ዲቴክት ማድረግ የሚያስችሉ ድክመቶች፣ መለያዎች፣ መፍትሄዎች፣ ወዘተ) ማውጣት፣ የተለያዩ ጥቃቶችን ማስተሳሰር፤
➢ የዲቴክሽን ሩል የመስራት ብቃት፤	➢ በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን (Hosts) ደረጃ ለተለያዩ የሳይበር ጥቃቶች የ correlation ሃሳብን በመተግበር የተለያየ አሴቶችን (assets) ያማከለ፣ ዜሮ false positive ያላቸው፣ ዉጤታማ፣ ወጪ ቆጣቢ እና ጠንካራ የዲቴክሽን ሩሎችን መስራት፣ false positive ላለባቸው ሩሎች ሁኔታውን ያገናዘበ ማስተካከያ ማድረግ፤
➢ ምላሽ መስጠት አቅም፤	➢ በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን (Hosts) ደረጃ ጥቃት የደረሰባቸውን ወይም ሊደርስባቸው የሚችሉ software እና/ወይም hardware ጉዳቱን በሚመልስ እና ጥቃቱ ተመልሶ በማያጠቃው መልኩ ምላሽ መስጠት፤
➢ የመሰነድ አቅም፤	➢ በየጊዜው የሚያጋጥሙ ተግዳሮቶች የተፈቱበትን እውቀት መሰነድ፤

የሥራ መደብ :- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ

ደረጃ: IV

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ስርተፍኬቶች
➢ ከደረጃ 4 በታች የተጠቀሱትን ኃላፊነቶች በብቃት ማከናወን መቻል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት መቆጣጠር፤	➢ ዌብላንጉች (ፒ.ኤች.ፒ፣ ኤሴ.ፒ፣ ኤች.ቲኤ.ምኤል፣ወዘተ) ➢ ኔትወርኪንግ ➢ Internet and cloud ➢ Internet programming ➢ ኔትወርክ ሴክዩሪቲ ➢ Operating system ➢ አድቫንስድ የሳይበር ጥቃት እውቀት፤ ➢ Network security monitoring	➢ በዲፖርትመንት/በቅርንጫፍ/ዲቪዥን ደረጃ የተሰሩ ስራዎችን ማረጋገጥ፤ ➢ በተቋም ደረጃ የተገጠሙ የዲቴክሽን የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በሙሉ ብቃት መጠቀም መቻል፣ስለተቋሙ ሲስተሞች አሰራር እና አጠቃላይ የኔትዎርክ እንቅስቃሴ (day-to-day activities, input and outputs, etc) በጥልቀት ማወቅ እና ከሳይበር ጥቃት አንፃር መረዳት፤ ➢ በተቋም ደረጃ የተገጠሙ የዲቴክሽን የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በመጠቀም በተቋም ደረጃ true positive ጥቃቶችን መለየትና የመጀመሪያ ደረጃ	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ፤	የመጀመሪያ ዲግሪ 3 እስከ 4 ዓመት ሁለተኛ ዲግሪ 1 እስከ 2 ዓመት አግባብነት ያለው የሥራ ልምድ	➢ Continuous monitoring certification (training or certifcation, **ወይም** ➢ Security essential **ወይም** ➢ Certified SOC analyst **ወይም** Certified

➢ በተሰጠው የስራ እቅድ መሰረት የራሱ እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ ከታች ለሚገኙ ባለሞያዎች ስልጠናዎችን ይሰጣል፤ ➢ በተቋም ደረጃ የሚገኙ የተለያዩ እሴቶችን ከፋፍሎ የሳይበር ጥቃት ዲቴክሽን/ሞኒተሪንግ ማከናወን፤ ➢ በተቋም ደረጃ የሳይበር ጥቃት አርቲፋክት መሰብሰብ፤ ➢ በተቋም ደረጃ የጥቃቶች አናሊሲስ በመስራት መረጃ ማቅረብ፤ ➢ አስተያየት እና ሪፖርት ማዘጋጀት፤ ➢ በተቋም ደረጃ ለጥቃቶች ተገቢውን ምላሽ መስጠት፤ ➢ በተቋም ደረጃ ላሉ ጥቃቶች ሩል እና/ወይም ስግኒቸር, IOC	➢ Network and host security detection, prevention and monitoring devices ➢ አድቫንስድ ኢንትሩዥን ዲቴክሽን፤ ➢ Threat hunting and artifact collection ➢ አድቫንስድ ኢንሲደንት ሃንድሊንግ፤ ➢ Advanced data and system recovery ➢ Advanced knowledge of log management and correlation ➢ Behavioral detection ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣እቅድ የማውጣት እና የመምራት እውቀት፤	analysis መስራት (የስራ መመሪያዎች /Working Manual/ መርሆች, procedures, policies መሰረት በማድረግ)፤ ➢ የተፈጠረውን ክስተት ምልክት ለሚያደርጉ ማንቂያ ደውሎች አዲስ የክስተት (incident)ትኬቶችን መፍጠር፤ ➢ በተቋም ደረጃ ሎግ፤ ኢቭንት፤ ትራፊክ፤ ወዘተ ላይ ዳታ /አርቲፋክት መሰብሰብ፤ ➢ በተቋም ደረጃ እንግዳ የሆነ እንቅስቃሴ በማየት አርቲፋክት ለይቶ መሰብሰብ፤ ➢ በተቋም ደረጃ ሪሶርስ (ራም፤ሲፒዩ፤ ባንድዊድዝ፤ወዘተ) አናሊሲስ፤ ➢ በተቋም ደረጃ በዲቴክሽን true positive ተብለው የተለዩ ጥቃቶችን የተሰበሰቡትን ዳታ/አርቲፋክት በመጠቀም ጠለቅ ያለ አናሊሲስ በመስራት የተቋሙን የሪፖርት መስፈርት ተከትሎ ሪፖርት እና ሪኮመንዴሽን ማምረት፤ ➢ በተቋም ደረጃ ለደረሱ ጥቃቶች ተገቢውን የምላሽ መስጠት ማከናወን፤ ➢ በተቋም ደረጃ የጥቃት አናሊሲስ በሚገኙ ዉጤቶች መሰረት የዲቴክሽን፣ፕሪቬንሽን እና ሞኒተሪንግ ሲስተሞችን ሩል እና/ወይም ስግኒቸር, IOC ማስተካከል እና አዳዲስ መጨመር፤ ➢ በተቋም ደረጃ የሚገኙ የተለያዩ እሴቶችን ለሞኒተሪንግ በሚያመች መልኩ መከፋፈል እና ሊደርሱ የሚችሉባቸውን የሳይበር			incident handler (training or certifcation, **ወይም** ➢ Certified intrusion analyst ቢኖር ይመረጣል፤

ማስተካከል እና አዳዲስ መጨመር፤ ➢ በተቋም ደረጃ የ vulnerability assessment ማካሄድና ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ በተቋም ደረጃ ለ False positive alerts የዲቴክሽን ሩል ማስተካከል፤ ➢ የሞኒተሪንግ ሥራ በተቋሙ እሴቶች ደረጃ ማስፋት፤ ➢ የ behavioral detection መሳሪያዎችን tune ማድረግ፤		ጥቃቶች መዘርዘር (scenarios) ከእሴቶቹ መገኘት በሚችሉ ዳታ መሰረት ለጥቃቶቹ ተገቢውን የዲቴክሽን ሩል መስራት፤ ➢ በተቋሙ ዉስጥ የሚገኙ የሳይበር ደህንነት ክፍተቶች መመዘኛ መሳሪያዎች በተቋም ደረጃ በተሰጠው የጊዜ ሰሌዳ እና ወሰን መሰረት vulnerability assessment ማካሄድ፤ ➢ በተቋም ደረጃ በvulnerability assessment ለተገኙ ክፍተቶች ተገቢውን ምላሽ መስጠት፤ ➢ በተቋም ደረጃ False positive ተብለው ለተለዩ alerts የዲቴክሽን ሩል ማስተካከል (if the rule is defective or generating false positive)፤ ➢ በተቋም ደረጃ ሞኒተር የሚደረጉ አዳዲስና ያልገቡ እሴቶችን ወደ ሞኒተሪንግ ሲስተምስ ማቀላቀል፤ ➢ በተቋሙ በ behavioral detection የሚሰሩ የሳይበር ጥቃት መከላከል መሳሪያዎችን የተለያዩ ጥቃቶችን በማየት እንደአስፈላጊነቱ tune ማድረግ፤ ➢ ከታች ባሉ ደረጃዎች የሚመጡ (escalated) ጥቃቶችን አናሊሲስ፣ ምላሽ የመስጠት፣ሩል የማስተካከል፣ ወዘተ ስራዎችን በትብብር መስራት፤ ➢ አናሊሲስ የተሰራባቸውን ጥቃቶች በተቋሙ/በቡድኑ የሪፖርት ቅርጸት			

		(format) መሰረት መሰነድ፣ በተጨማሪም የተስተካከሉ ወይም አዳዲስ የተጨመሩ ሩሎችን ከነዝርዝራቸው በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ፤			

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ ጥቃቶችን ዲቴክት ማድረግ፣ rule based እና behavioral፤	➢ የሳይበር ጥቃቶችን መለያ መንገዶችን በማወቅ ጥቃቶችን ዲቴክት ማድረግ፣ ከቋሚ ሩሎች በተጨማሪ በባህሪ ላይ የተመሰረተ ዲቴክሽን ማድረግ መሳሪያዎችን tune በማድረግ እንደ ተቋሙ የኔትወርክ ፍሰት እና የእሴቶች (assets) እንቅስቃሴ፤
➢ False positive እና true positive የሳይበር ጥቃቶችን መለየት፤	➢ በተቋም ደረጃ የሚታዩ ትክክለኛ ጥቃቶችን በመለየት ሞኒተር ማድረግ፤
➢ አርቲፋክት መሰብሰብ፤	➢ በተቋም ደረጃ ጥቃቶች ላይ ጥልቅ አናሊሲስ ሊያሰሩ የሚችሉ የተለያዩ አርቲፋክቶችን የሚቀመጡበትን ቦታዎች ማወቅ እና መሰብሰብ፤
➢ አናሊሲስ/ትንተና፤	➢ በተቋም ደረጃ የተሰበሰቡ አርቲፋክቶችን ከተለያዩ የጥቃቱ ሁኔታዎች፣ የሲስተሞች አቋም፣ ወዘተ ጋር በማገናኘትና በማገናዘብ ስለ ጥቃቱ የተለያዩ ዝርዝሮችን (ምን አይነት ጥቃት ነው፣ አላማው ምንድነው፣ ምን ጉዳት አስከተለ፣ የተጠቀማቸው ዘዴዎች፣ ጥቃቱን መከላከልና ዲቴክት ማድረግ የሚያስችሉ ድክመቶች፣ መለያዎች፣ መፍትሄዎች፣ ወዘተ) ማውጣት፣ የተለያዩ ጥቃቶችን ማስተሳሰር፤
➢ የዲቴክሽን ሩል የመስራት ብቃት፤	➢ በተቋም ደረጃ ለተለያዩ የሳይበር ጥቃቶች የ correlation ሃሳብን በመተግበር የተለያየ አሴቶችን (assets) ያማከለ፣ ዜሮ false positive ያላቸው፣ ዉጤታማ፣ ወጪ ቆጣቢ እና ጠንካራ የዲቴክሽን ሩሎችን መስራት፣ false positive ላለባቸው ሩሎች ሁኔታውን ያገናዘበ ማስተካከያ ማድረግ፤

➢ ምላሽ መስጠት አቅም፤	➢ በተቋም ደረጃ ጥቃት የደረሰባቸውን ወይም ሊደርስባቸው የሚችሉ software እና/ወይም hardware ጉዳቱን በሚመልስ እና ጥቃቱ ተመልሶ በማያጠቃው መልኩ ምላሽ መስጠት፤

የሥራ መደብ መጠሪያ፡- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ

ደረጃ፡ IV

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት
➢ ከደረጃ 5 በታች የተጠቀሱትን ኃላፊነቶች በብቃት ማከናወን መቻል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት መቆጣጠር፤ ➢ በተቀመጠው የስራ እቅድ መሰረት የራሱ እቅድ እና	➢ አፕሊኬሽን ሀኪንግ ➢ አድቫንስድ ኔትወርክ ሴክዩሪቲ እና ሀኪንግ ➢ Advanced Operating system ➢ አድቫንስድ የሳይበር ጥቃት እውቀት ➢ አድቫንስድ ኢንሲደንት ሃንድሊንግ ➢ አድቫንስድ ኢንትሩዥን አናሊሲስ ➢ Advanced data and system recovery ➢ Secure code development	➢ በተቋም ደረጃ የተሰሩ ስራዎችን ማረጋገጥ፤ ➢ በተቋሙ ዉስጥ የሚከሰቱ ነገር ግን ዲቴክት ያልተደረጉ (false negative)፤ አይነት ጥቃቶችን ማግኘት፣የተሰበሰቡትን ዳታ/አርቲፋክት በመጠቀም ጠለቅ ያለ አናሊሲስ በመስራት ምላሽ መስጠት፣ ➢ ዲቴክት ያልተደረገበትን ምክንያት በመለየት የዲቴክሽንሩል/ሲግኔቸር/behavioral መንገዶችን ማስቀመጥና መተግበር፤ ➢ በተቋሙ በሳይበር ጥቃት	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ፤	የመጀመሪያ ዲግሪ 4 እስከ 5 ዓመት ሁለተኛ ዲግሪ 2 እስከ 3 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Certifed incident analyst **ወይም** ➢ Advanced incident handling (training or certifcation, **ወይም** ➢ Certified Data Recovery Professional (training or certifcation, **ወይም**

አተገባበር ሂደት ያወጣል፤ ➢ ከታች ለሚገኙ ባለሞያዎች ስልጠናዎችን ይቀርጻል፣ይሰጣል፤ ➢ በየጊዜው በተቋሙ ውስጥ የሚከሰቱ false negative ጥቃቶችን ዲቴክት ማድረግ፣ ምላሽ መስጠት እና ተገቢውን ዲቴክት ማድረጊያ መንገዶችን ማስቀመጥ እና መተግበር፤ ➢ የሳይበር ሴኪዩሪቲ እቃዎችንና መሳሪያዎችን Maintenance እና configuration ስራዎችን መስራት፤ ➢ እንደአስፈላጊነቱ ልዩ ጥቃቶችን ምላሽ መስጠት የሚያስችሉትን መሳሪያዎችን (mini-tools) በማበልፀግ ምላሽ መስጠት፤ ➢ ለ critical፣ከፍተኛ ጉዳት ለደረሰባቸው ልዩ እና ትኩረት ለሚያስፈልጋቸው እሴቶች በጥንቃቄ ምላሽ መስጠት፤ ➢ ደረጃውን የጠበቀ እና	➢ Advanced threat hunting and artifact collection ➢ Advanced log management and correlation ➢ Behavioral detection, machine learning የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣እቅድ የማውጣት እና የመምራት እውቀት፤	መከላከል ዘርፍ ያሉ ሃብቶችን የአገልግሎት ዘመናቸውን መሰረት ያደረገ የጥገናና የሰርቪስ ክትትል (ሲበላሹም ጭምር)፣በተጨማሪም እንደአስፈላጊነቱ የተለያዩ የማስማማት ስራዎችን መስራት፤ ➢ የተለየ ምላሽ ለሚያስፈልጋቸው የሳይበር ጥቃቶች እንደአስፈላጊነቱ የራስንም mini-tool በመስራት ምላሽ መስጠት፤ ➢ በተቋሙ ደረጃ sensitive ለሆኑ እሴቶች በተለይም critical ተብለው ለተለዩ፣ወደ ሥራ መልሶ ለማስገባት አስቸጋሪ አይነት ጥቃት ለደረሰባቸው እና በትላልቅ በዉስብስብ ቱሎች እና ሜተድ ምላሽ ለሚሰጥባቸው ጥንቃቄ የተሞላበት ምላሽ መስጠትና ችግሩን መፍታት፤ ➢ ለሳይበር ጥቃት አናሊሲስ የሚረዱ ላቦራቶሪዎችን የተለያዩ አገር አቀፍ እና ዓለም አቀፍ ስታንዳርዶችን በማየት ዲዛይን ማድረግ እና መተግበር (as per the organization's capacity)፤ ➢ በተቋሙ ዉስጥ የሚደርሱ እና			➢ Certified secure programmer (coder) **ወይም** ➢ CEH SIEM with tactical analytics ቢኖር ይመረጣል፤

የተቋሙን ደረጃ ያገናዘበ የአናሊሲስ ላቦራቶሪ መተግበሪያ፤		ሊደርሱ የሚችሉ ጥቃቶችን የተዘረጋውን ላቦራቶሪ በመጠቀም simulate አድርጎ ደሞ ማዘጋጀት፤ ➢ በየጊዜው በአገር አቀፍ እና ዓለም አቀፍ ደረጃ የሚታዩ የሳይበር ጥቃቶችን ከተለያዩ ምንጮች በማየት የጥቃቶችን አዝማሚያ መተንበይ፤			

የመወዳደሪያ አቅሞች

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ False negative detection	➢ ዲቴክት ከተደረጉ ጥቃቶች ወጣ ብሎ በተቋሙ ዉስጥ አየደረሱ ያሉ ያልታወቁ ጥቃቶችን መለየት እና ዲቴክት እንዲደረጉ ማስቻል፤
➢ Threat hunting	➢ በተቋም ደረጃ ያሉ አሴቶችን በደንብ በማወቅ የሳይበር ጥቃቶችን ሊያሳዩ የሚችሉ ቦታዎችን በመመርመር ጥቃቶችን ማግኘት፤
➢ አናሊሲስ	➢ በተቋም ደረጃ የተሰበሰቡ አርቲፋክቶችን ከተለያዩ የጥቃቱ ሁኔታዎች፣ የሲስተሞች አቋም፣ ወዘተ ጋር በማገናኘትና በማገናዘብ ስለ ጥቃቱ የተለያዩ ዝርዝሮችን (ምን አይነት ጥቃት ነው፣ አላማው ምንድነው፣ ምን ጉዳት አስከተለ፣ የተጠቀማቸው ዘዴዎች፣ ጥቃቱን መከላከልና ዲቴክት ማድረግ የሚያስችሉ ድክመቶች፣ መለያዎች፣ መፍትሄዎች፣ ወዘተ) ማውጣት፣ የተለያዩ ጥቃቶችን ማስተሳሰር፤
➢ Attack pattern, trend and correlation	➢ የጥቃቶችን ድግግሞሽ፣ አዝማሚያ (trends)፣ንድፍ (pattern) እና ሌሎች ዝርዝሮችን በማየት ማዛመድ (relate) እና correlate ማድረግ፤

➢ ምላሽ መስጠት አቅም	➢ የተለየ ምላሽ ለሚያስፈልጋቸው የሳይበር ጥቃቶች እንደ አስፈላጊነቱ የራስንም mini-tool በመስራት ምላሽ መስጠት ➢ በተቋሙ ደረጃ sensitive ለሆኑ አሴቶች በተለይም critical ተብለው ለተለዩ፣ ወደ ሥራ መልሶ ለማስገባት አስቸጋሪ አይነት ጥቃት ለደረሰባቸው እና በትላልቅ በዉስብስብ ቱሎች እና ሜተድ ምላሽ ለሚሰጥባቸው ጥንቃቄ የተሞላበት ምላሽ መስጠትና ችግሩን መፍታት፤

የሥራ መደብ :- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ
ደረጃ፡ VI

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራልምድ	ሰርተፍኬቶች
➢ ከደረጃ 6 በታች የተጠቀሱትን ኃላፊነቶች በብቃት ማከናወን መቻል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚወጡ እቅዶችን ከተቋሙ እና ከክፍሉ እቅድ አንጻር ይገመግማል፣ ያረጋግጣል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት	➢ Advanced Operating system ➢ አድቫንስድ ኔትወርክ ሴኪዩሪቲ እና ሀኪንግ፤ ➢ አድቫንስድ አፕሊኬሽን	➢ በደረጃ 5 የተሰሩ ስራዎችን ማረጋገጥ፣አስፈላጊ ሲሆን ምስራዎቹን አብሮ መስራት፤ ➢ በተቋሙ ዉስጥ ሊደርሱ የሚችሉ የ APT (Advanced Persistent Threats) ጥቃቶችን አስቀድሞ ዲቴክት ማድረግ እና ከደረሱም በኃላ የአናሊሲስ እና ምላሽ መስጠት ስራዎችን በጥንቃቄ	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ የመጀመሪያ ወይም ሁለተኛ ዲግሪ፤	የመጀመሪያ ዲግሪ 6 እስከ 7 ዓመት ሁለተኛ ዲግሪ 4 እስከ 5 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ Advanced Application hacking ➢ Certified incident analyst (training or certifcation, **ወይም** ➢ Advanced

መቆጣጠር፤ ➢ በተሰጠው የስራ እቅድ መሰረት የራሱ እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ ከታች ለሚገኙ ባለሞያዎች ስልጠናዎችን ይቀርጻል፣ይሰጣል፤ ➢ ተቋሙ ባስቀመጠው እቅድ ወይም በየ 6 ወሩ የቴክኒካል ሪፖርት ለበላይ አመራር ያቀርባል። ➢ የ APT (Advanced Persistent Threats) ጥቃቶችን ዲቴክት ማድረግ፣አናሊሲስ መስራት እና ምላሽ መስጠት፤ ➢ በተቋሙ ደረጃ የሳይበር ጥቃቶች ቅድመ መከላከል ዝግጅት ማድረግ፤ ➢ ለሳይበር ደህንነት ክስተት እና ክትትል ቡድን የሚጠቅሙ መሳሪያዎችን እንደስፈላጊነቱ ማበልፀግ፤ ➢ የ open source እና commercial መሳሪያዎችን በጥንቃቄ መምረጥና ምክረ ሃሳብ ማቅረብ፣ open source የሆኑትን የበላይ አመራር በማማከር መተግበር፤ ➢ የተቋሙን የዲቴክሽን	ሀኪንግ ➢ አድቫንስድ የሳይበር ጥቃት እውቀት ➢ አድቫንስድ ኢንሲደንት ሃንድሊንግ ➢ አድቫንስድ ኢንሲደንት አናሊሲስ ➢ Advanced data and system recovery ➢ Secure code development ➢ Advanced threat hunting and artifact collection ➢ Advanced log management and correlation ➢ Behavioral detection, machine learning ➢ Attack techniques and	ማከናወን፤ ➢ በተቋሙ ዉስጥ ለቅድመ ጥቃት ዲቴክሽን እና መከላከል፣ጥቃት ከተከሰተም በኋላ ለአናሊሲስ የሚረዱ የኮንፊገሬሽንና ዝግጅት (Forensic readiness, IOA) ስራዎችን መስራት፣በተጨማሪም ለዚህ ሥራ የሚረዳ ላቦራቶሪ እንደአስፈላጊነቱ ማዘጋጀት፤ ➢ በተቋሙ ዉስጥ የተለያዩ ለዲቴክሽን፣ artifact collection, ፕሪቬንሽን እና አናሊሲስ ስራዎች የሚጠቅሙ መሳሪያዎችን ማበልፀግ (ከበላይ አመራር ጋር በመነጋገር)፤ ➢ ከአቅም በላይ የሆኑ የሳይበር ጥቃቶች በሚያጋጥሙ ጊዜ ለ national cert/sectorial cert ቡድን escalate ማድረግ እና አብሮ መስራት (አናሊሲስ እና ምላሽ መስጠት)፤ ➢ ከ national cert/sectorial cert ቡድን የሚወጡ የሳይበር ጥቃት መለያ (ሲግኒቸር፣ሩል፣ IoC፣ ወዘተ) እና መፍትሄዎችን መቀበል እና በየደረጃው ከሚመለከታቸው የቡድን አጋሮች ጋር በመሆን መተግበር፤			incident handling (training or certifcation, **ወይም** ➢ Certified Data Recovery Professional **ወይም** ➢ Certified secure programmer (coder) **ወይም** ➢ GIAC Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses **ወይም** ➢ GIAC Advanced Incident Response,

የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎች መመዘን እና መሞከር፣ ዉጤቱን ሪፖርት ማድረግ፤ ➢ ከ national cert/sectorial cert ቡድን ጋር ግንኙነት በማድረግ ስራዎችን መስራት፤ ➢ በቡድን Capture-The-Flag ጨዋታዎችን design አድርጎ ማጫወት፤ ➢ የቡድኑን እውቀቶች የሚያጋራ ሲስተም ወይም ሌሎች መንገዶች ማዘጋጀት፤	tools modeling (from defense perspective) ➢ Attack patterns recognition and correlation ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣ እቅድ የማውጣት እና የመምራት እውቀት፤	➢ በየጊዜው አጠቃላይ የተቋሙን የኔትዎርክ እና ሲስተሞች አቋም በማየት የሳይበር ክፍተቶችን በመለየት ለሳይበር ጥቃት ዲቴክሽን እና አናሊሲስ የሚረዱ open source እና commercial መሳሪያዎችን በጥንቃቄ መምረጥ (የአገር አቀፍ ምክር በማየት ጭምር) እና መተግበር፣ የሚገዙ መሳሪያዎችን ለበላይ አካል ማቅረብ፤ ➢ በተቋሙ ዉስጥ የሚገጠሙ open source እና commercial የዲቴክሽን፣ የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን በተቋሙ በሚወጡ የመመዘኛ እና የመሞከሪያ መስፈርቶች መሰረት መመዘን እና መሞከር፣ ዉጤቱን ሪፖርት ማድረግ፤ ➢ የሳይበር ደህንነት ክስተት እና ክትትል ቡድንን የመከላከልችሎታ (skill) ሊያሳድጉ የሚችሉ የተለያዩ ጨዋታዎችን (Capture-The-Flag) ላቦራቶሪ በመጠቀም simulate አድርጎ መተግበር እና ማጫወት፤ ➢ በቡድኑ ዉስጥ የሚሰሩ ስራዎችንና ሌሎች እውቀቶችን			Threat Hunting, and Digital Forensics (training or certifcation, **ወይም** ➢ GIAC Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response ➢ SANS Advanced Memory Forensics &Threat Detection **ወይም** ➢ Certified Advanced Persistent Threat Analyst (training or

		ማስቀመጥ የሚችል knowledge base ሲስተም ማዘጋጀት፤ ➢ አናሊሲስ የተሰራባቸውን ጥቃቶች፣ የተሰጡ ምላሾች፣ ሌሎች ስራዎችን በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ፤			certifcation, ቢኖር ይመረጣል፤
የመወዳደሪያ አቅሞች	**ማብራሪያ**				
➢ Threat hunting	➢ በተቋም ደረጃ ያሉ አሴቶችን በደንብ በማወቅ ለብዙ ጊዜያት ሳይታወቁ ተደብቀው ሊቀመጡ የሚችሉ ስጋቶችን በጥናት ማግኘት፤				
➢ Attackers tools, techniques, tactics and defense mechanisms	➢ ጥቃት አድራሾች የሚጠቀሙባቸውን የተለያዩ መሳሪያዎች፣ ዘዴዎች፣ መንገዶችና ለነዚህ የሚሆኑ ውጤታማ የመከላከያ መንገዶች እውቀት (በዓለም ላይ የሚታወቁና የራሱንም መፍጠር)፤				
➢ Analysis	➢ በተቋም ደረጃ የተሰበሰቡ አርቲፋክቶችን ከተለያዩ የጥቃቱ ሁኔታዎች፣ የሲስተሞች አቋም፣ ወዘተ ጋር በማገናኘትና በማገናዘብ ስለ ጥቃቱ የተለያዩ ዝርዝሮችን (ምን አይነት ጥቃት ነው፣ አላማው ምንድነው፣ ምን ጉዳት አስከተለ፣ የተጠቀማቸው ዘዴዎች፣ ጥቃቱን መከላከልና ዲቴክት ማድረግ የሚያስችሉ ድክመቶች፣ መለያዎች፣ መፍትሄዎች፣ ወዘተ) ማውጣት፣ የተለያዩ ጥቃቶችን ማስተሳሰር፤				
➢ Coding	➢ ለኦፕሬቲንግ ሲስተም የቀረቡ (less encapsulation) የፕሮግራሚንግ ቋንቋዎችን በመጠቀም የቡድኑን ሥራ ሊያግዙ የሚችሉ መሳሪያዎችን ደህንነቱ በተጠበቀ መልኩ ማበልፀግ፤				

የሥራ መደብ ፡- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ
ደረጃ፡ VII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ዝግጅት	ሥራ ልምድ	ሰርተፍኬት
➢ ከደረጃ 7 በታች የተጠቀሱትን ኃላፊነቶች በብቃት ማከናወን መቻል፤ ➢ ከደረጃው በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ያቅዳል፣ ይመራል፤ ➢ ከሱ በታች ባሉ ደረጃዎች	➢ Advanced incident handling ➢ Advanced network security ➢ የምዘና መስፈርቶችን (Checklists)፣የአሰራር ሂደቶችን (Procedures)	➢ በደረጃ 6 የተሰሩ ስራዎችን ማረጋገጥ፣አስፈላጊ ሲሆን ስራዎችን አብሮ የመስራት፤ ➢ ለሳይበር ደህንነት ክስተት እና ክትትል ቡድን የሞኒተሪንግ፣አርቲፋክት መሰብሰብ፣አናሊሲስ እና	በኢንፎርሜሽን ሳይንስ፣ ኮምፒውተር ሳይንስ፣ ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን	የመጀመሪያ ዲግሪ 7 እስከ 8 ዓመት ሁለተኛ ዲግሪ 5 እስከ 6 ዓመት	➢ Certified intrusion analyst (training or certifcation, **ወይም** Advanced incident handling

የሚሰሩ ስራዎችን ጥራት መቆጣጠር፤ ➢ በተቀመጠው የክፍሉ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ Process እና Procedures መቅረጽ እና እንዲተገበሩ ማድረግ፤ ➢ የዉስጥ እና የውጪ አገር ስልጠናዎችን መቅረጽና ሃሳብ ማቅረብ፤ ➢ የዲቴክሽን፣ የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን የይለፍ ቃል (password) ማስተዳደር፤ ➢ በቡድኑ ዉስጥ ያሉ ስራዎችን የሚያሰሩ የተለያዩ የጊዜ ሰሌዳዎችን ማውጣት፣ በየጊዜውም መከለስ (24/7 ለመስራት የሚያስችል ጭምር)፤ ➢ የተቋሙን ጥሪቶች(assets) በተለያየ መስፈርት መከፋፈል፤ ➢ የቡድኑን የስራዎች ጥራት መቆጣጠርና የማሻሻያ ምክረ ሃሳቦችን ማቅረብ፤	እና ዘዴዎችን (Methodologies) እውቀት; ➢ SOC management ➢ System administration and HR management ➢ Product evaluation knowledge ➢ Cyber threat, techniques and defense models ➢ በሃገር አቀፍ ደረጃ የወጡ መመሪያዎች፣እና ደረጃዎችን በጥልቀት ማወቅ፤ ➢ ተቋሙ የሚከተላቸውን እና የሚገደድባቸውን ደረጃዎች ማወቅ እና መረዳት፤ ➢ የአሰራር ጥራት ደረጃዎችን እና የአሰራር ጥራት መመዘኛ መስፈርቶችን የመከታተል ዕውቀት፤ ➢ የአገር እና አለም አቀፍ ደረጃ የወጡ ስታንዳርዶችን፣ወዘተ	ምላሽ መስጠት ስራዎች የሚያገለግሉ process እና procedures መቅረጽ እና እንዲተገበሩ ማድረግ፤ ➢ ለሳይበር ደህንነት ክስተት ክትትል ቡድን የሚጠቅሙ የተለያዩ የውስጥ እና የውጪ አገር ስልጠናዎችን መቅረጽና ሃሳብ ማቅረብ፤ ➢ የvulnerability assessment በየደረጃው የሚሰራበትን የጊዜ ሰሌዳ ማውጣት እና መተግበሩን ማረጋገጥ፤ ➢ በተቋም ደረጃ የተገጠሙና የሚገጠሙ የዲቴክሽን፣ የፕሪቬንሽን የvulnerability assessmentና የሞኒተሪንግ መሳሪያዎችን የይለፍ ቃል (password) ማስተዳደር፣ በተጨማሪም በየደረጃው ያሉ ሰራተኞች የሚመለከታቸው ሲስተሞችን መመደብ፤ ➢ በግዢ ወይም በጥገና ምክንያት ከ product vendors ጋር የሚደረጉ ግንኙነቶችን በተቋሙ	ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ፤	አግባብነት ያለው የሥራ ልምድ፤	(training or certifcation **ወይም** ➢ Implementing and Auditing the Critical Security Controls **ወይም** ➢ Defensible Security Architecture and Engineering **ወይም** ➢ Security Leadership Essentials For Managers(training or certifcation **ቢኖር ይመረጣል**፤

➢ ከ product vendors ጋር ግንኙነቶችን ማድረግ፤ ➢ የሳይበር ጥቃት ሪፖርቶችን ማዘጋጀት እና ማቅረብ፤ ➢ የተቋሙን የዲቴክሽን፣ የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎች የመመዘኛ እና የመሞከሪያ መስፈርቶችን ማውጣትና መተግበራቸውን ማረጋገጥ፤ ➢ የተቋሙን Disaster recovery ዕቅድ ከሚመለከታቸው አካላት ጋር በመሆን መተግበር፤ ➢ ከታች ለሚገኙ ባለሙያዎች ስልጠናዎችን ይቀርጻል፣ ይሰጣል፤	ማወቅ እና መረዳት፤ ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣እቅድ የማውጣት እና የመምራት እውቀት፤	ስታንዳርድ መሰረት በበላይነት መምራት (ከበላይ አመራር በሚሰጥ አቅጣጫ)፤ ➢ የሳይበር ጥቃቶች ዲቴክሽን፣አናሊሲስ እና ምላሽ መስጠት ስራዎችን በ 24/7 ለመስራት የሚያስችል የጊዜ ሰሌዳ ያወጣል፣ በየጊዜውም ይከልሳል፤ ➢ የተቋሙን assets ከሳይበር ጥቃት ተጋላጭነት እና ለስራ ወሳኝ አስፈላጊነት (business critical) አንፃር ከሌሎች ከሚመለከታቸው ቡድኖች ጋር በመሆን መከፋፈል እና ከሱደረጃ በታች ላሉት ማስገንዘብ (ከበላይ በሚሰጥ አቅጣጫ መሰረት)፤ ➢ የሞኒተሪንግ፣አናሊሲስ እና ምላሽ መስጠት ሪፖርቶችን በተፈለገው መንገድ ለበላይ አካል ማቅረብ፤ ➢ በተቋም ደረጃ በሚወጣ የሥራዎች ጥራት መለኪያ እና ማሻሻያ መስፈርት መሰረት ስራዎችን			

		መለካትና የሚሻሻሉበትን ምክረ ሃሳብ አቅርቦ መተግበሩን መከታተል፤ ➢ በተቋሙ ዉስጥ የሚገጠሙ open source እና commercial የዲቴክሽን የፕሪቬንሽንና የሞኒተሪንግ መሳሪያዎችን የመመዘኛ እና የመሞከሪያ መስፈርቶችን ማውጣትና መተግበራቸውን በየጊዜው ማረጋገጥ፣ በየጊዜው መከለስ፤ ➢ ተቋሙን በከፍተኛ ሁኔታ የሚጎዳ ጥቃት በሚያጋጥም ጊዜ የተቋሙን Disaster recovery ዕቅድ ከሚመለከታቸው አካላት ጋር በመሆን መተግበርና የተቋሙን የስራ ሂደት ማስቀጠል መቻል፤ ➢ በተቋሙ የሚወጡ ለቡድኑ የሚያገለግሉ የተለያዩ ምርጥ ተሞክሮዎችን፣ አዳዲስ አካሄዶችን፣ምክረ ሃሳቦችን እንደ የሁኔታው ከሚመለከታቸው አካላት ጋር በመሆን መተግበር፤ ➢ የተቋሙን እና የአገር አቀፍ			

		እንዳስፈላጊነቱም ዓለም አቀፍ ስታንዳርዶችን በማየት የቡድኑን የተለያዩ ስራዎችን መሰነድ የሚያስችሉ የሪፖርት ቅርጸቶች (formats) ማዘጋጀት፤ ➢ ሁሉንም ስራዎችን በተቋሙ/በቡድኑ የሪፖርት ቅርጸት (format) መሰረት መሰነድ፤			

የመወዳደሪያ አቅሞች	ማብራሪያ (Description)
➢ Process, proceduresእና methodologies የመቅረጽ ብቃት፤	➢ የተቋሙን ሁኔታ (እንቅስቃሴ) ከሳይበር ደህንነት ጋር በማያያዝ ለሳይበር ክስተት ደህንነት አስተዳደር ቡድን የተለያዩ ስራዎችን መስራት የሚያስችሉ Process, proceduresእና methodologies መቅረጽ፤
➢ Attackers tools, techniques, tactics and defense mechanisms፤	➢ ጥቃት አድራሾች የሚጠቀሙባቸውን የተለያዩ መሳሪያዎች፣ ዘዴዎች፣ መንገዶችና ለነዚህ የሚሆኑ ውጤታማ የመከላከያ መንገዶች እውቀት (በዓለም ላይ የሚታወቁና የራሱንም መፍጠር)፤
➢ ጥራት የመመዘን ብቃት፤	➢ የአሰራር ጥራት ደረጃዎችን እና የአሰራር ጥራት መመዘኛ መስፈርቶችን ማበልጸግ እና የመከታተል አቅም፤
➢ ሰውና ሀብት የማስተዳደር	➢ የቡድኑን የዕለት ተዕለት እንቅስቃሴ በብቃት የሚያሰሩ ሁኔታዎችን (technical እና non-technical) ፈጥሮ

ብቃት፤	ማስተዳደር፤
➢ ምክረ ሃሳብ የመተግበር ብቃት፤	➢ በተቋሙ የሚወጡ ለቡድኑ የሚያገለግሉ የተለያዩ ምርጥ ተሞክሮዎችን፣ አዳዲስ አካሄዶችን፣ ምክረሃሳቦችን እንደ የሁኔታው ከሚመለከታቸው አካላት ጋር በመሆን መተግበር፤
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት	➢ ቡድኑ የሚያስፈልጉትን የአገር ዉስጥና የውጭ ግንኙነቶች በውጤታማነት ማካሄድ፤

የሥራ መደብ ፡- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ
ደረጃ፡ VIII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ስርተፍኬት

➢ ከደረጃ 7 በታች የተጠቀሱትን ኃላፊነቶች በብቃት ማከናወን መቻል፤ ➢ የተቋሙን የሳይበር ደህንነት ክስተት አስተዳደር አጠቃላይ ስራ እና አተገባበር ስልታዊ (strategic) እቅድ ያዘጋጃል፣ ይመራል፤ ➢ ከሱ በታች ባሉ ደረጃዎች የሚሰሩ ስራዎችን ጥራት መቆጣጠር፤ ➢ በተቀመጠው የክፍሉ እቅድ መሰረት የራሱን እቅድ እና አተገባበር ሂደት ያወጣል፤ ➢ በአገር አቀፍ እና በተቋሙ ደረጃ የሳይበር ሴኪዩሪቲ ፖሊሲዎች ማውጣት ላይ መሳተፍ፤ ➢ በየጊዜው ለተቋሙ የተለያዩ የሳይበር ጥቃት መከላከያ ሞዴሎችንና ዲዛይኖችን መቅረፅ እና ማቅረብ፤ ➢ የቡድኑን ስራዎች ጥራት መለኪያና ማሻሻያ መስፈርቶችን ከነአተገባበራቸው መቅረፅ፤ ➢ የቡድኑን የኮምዩኒኬሽን ስታንዳርድ መቅረፅ፤	➢ Advanced incident handling ➢ Advanced network security ➢ መምራት እና ስልታዊ እቅዶችን ፖሊሲዎችን የማውጣት እውቀት፤ ➢ ስልጠና የመስጠት እና የመቅረጽ እውቀት፤ ➢ በተቋም ደረጃ የአሰራር ሂደቶችን፣ ዘዴዎችን (Methodologies)፣ የምዘና መስፈርቶችን መገንዘብና አዲስ የመፍጠር እውቀት፤ ➢ የአገር እና አለም አቀፍ ደረጃ የወጡ ስታንዳርዶችን፣ወዘተ ማወቅ እና መረዳት ➢ Building and managing SOC ➢ Asset classification and management, risk assessment	➢ በደረጃ 7 የተሰሩ ስራዎችን ማረጋገጥ፣አስፈላጊ ሲሆንም ስራዎቹን አብሮ የመስራት፤ ➢ ከ national cert/sectorial cert ቡድን እና/ወይም በተቋሙ ውስጥ ካሉ ሌሎች ቡድኖች ጋር በመሆን ሳይበር ሴኪዩሪቲን በተመለከተ የሚወጡ ፖሊሲዎች ላይ የመሳተፍ፤ ➢ በየጊዜው የዓለም አቀፍ እና አገር ውስጥ የሳይበር አዝማሚያ (trends) በመገንዘብ የተለያዩ የሳይበር ጥቃት መከላከያ ሞዴሎችንና ዲዛይኖችን የአገሪቷን የሳይበር ማአቀፍ እና የተቋሙን ፖሊሲዎች መሰረት ባደረገ መልኩ መቅረፅ እና ማቅረብ፤ ➢ በተቋሙ የተከሰቱ ጥቃቶችን እና መከላከያ መንገዶችን ለተቋሙ ሰራተኞች፣ሚዲያ ተቋማት፣ ለተለያዩ የአገሪቷ ባለስልጣናት፣ ወዘተ ማቅረብ አስፈላጊ በሚሆንበት ጊዜ ማቅረብ (ከበላይ አመራሮች ጋር በመነጋገር)፤ ➢ ለሳይበር ደህንነት ክስተት ክትትል ቡድን የሞኒተሪንግ፣አርቲፋክት መሰብሰብ፣አናሊሲስ፣ምላሽ መስጠት እና ማበልፀግ ስራዎችን	በኢንፎርሜሽን ሳይንስ፣ኮምፒውተር ሳይንስ፣ኤሌክትሪካል ኢንጂነሪንግ፣ ኮሙኒኬሽን ኢንጂነሪንግ ወይም ተዛማጅ የት/ት መስክ፤	የመጀመሪያ ዲግሪ 8 እስከ 9 ዓመት ሁለተኛ ዲግሪ 6 እስከ 7 ዓመት አግባብነት ያለው የሥራ ልምድ፤	➢ CISSP (training or certifcation, **ወይም** ➢ CISM **ወይም** ➢ Security Strategic Planning, Policy, and Leadership(training or certifcation, **ወይም** ➢ Certified Security Leadership Officer (CSLO) **ወይም** ➢ Law of Data Security and Investigations **ወይም** ➢ Security Expert Certification ቢኖር ይመረጣል፤

➢ የተቋሙን Disaster recovery ዕቅድ ከሚመለከታቸው ቡድኖች ወይም አካላት ጋር በመሆን ማዘጋጀት፤ ➢ የተቋሙን አጠቃላይ የአሰራር ሂደት በማጥናት ለቡድኑ ምርጥ ተሞክሮዎችን እና አዳዲስ አካሄዶችን እና ምክረ ሃሳቦችን ያቀርባል፣ ይተገብራል፤ ➢ በተቋሙ የቡድኑን የአጭርና የረጅም ጊዜ ዕቅድ እና ሪፖርት ያቀርባል፤ ➢ ከሌሎች ክፍሎች እና ተቋማት ጋር እንደ አስፈላጊነቱ ግንኙነት ያደርጋል፤ ➢ ከታች ለሚገኙ ባለሙያዎች ስልጠናዎችን ይቀርጻል፣ ይሰጣል፤	➢ የአመራር እውቀት ➢ Cyber threat, techniques and defense models, designing new models with different paradigms ➢ የአፈጻጸም ደረጃን ለመለካት የሚያስፈልጉ መስፈርቶች፣ መተግበሪያዎች እና ዘዴዎች፣እቅድ የማውጣት እና የመምራት እውቀት፤	ጥራት ሊለኩ እና ሊያሻሽሉ የሚችሉ መስፈርቶችንና አተገባበራቸውን በየጊዜው ማዘጋጀት (አለም አቀፍ እና አገር አቀፍ ስታንዳርዶችን በመጠቀም)፤ ➢ የተቋሙን ጥሪቶች(assets) መከፋፈያ መስፈርቶች ከተለያየ እይታ አንፃር ማውጣት እና መተግበራቸውን ማረጋገጥ (እንዳስፈላጊነቱ መከለስ)፤ ➢ የሳይበር ክስተት አስተዳደር ቡድን ከተቋሙ ውስጥ ያሉ ቡድኖች፣ከ national /sectorial ቡድን፣ከአገር ዉስጥ እና ዉጪ vendors ጋር የሚያደርገውን የስራ ግንኙነቶች የሚመራ ስታንዳርድ ማዘጋጀት፣ በየጊዜው እንደ አስፈላጊነቱ መከለስ (በአገር አቀፍ ደረጃ የሚወጣ ስታንዳርድ ካለ እሱን ያማከለ)፤ ➢ ከባለ ድርሻ አካላትጋር ግንኙነት ማድረግ ➢ የተቋሙን Disaster recovery ዕቅድ ከሚመለከታቸው ቡድኖች ወይም አካላት ጋር በመሆን ማዘጋጀት፣በየጊዜው እንደ አስፈላጊነቱ መከለስ፤ ➢ አጠቃላይ የቡድኑን ስራዎች፣			

ብቃት፤	ማስተዳደር፤
➢ ምክረ ሃሳብ የመተግበር ብቃት፤	➢ በተቋሙ የሚወጡ ለቡድኑ የሚያገለግሉ የተለያዩ ምርጥ ተሞክሮዎችን፣ አዳዲስ አካሄዶችን፣ ምክረሃሳቦችን እንደ የሁኔታው ከሚመለከታቸው አካላት ጋር በመሆን መተግበር፤
➢ የግንኙነት እና ተባብሮ የመስራት ብቃት	➢ ቡድኑ የሚያስፈልጉትን የአገር ዉስጥና የውጭ ግንኙነቶች በውጤታማነት ማካሄድ፤

የሥራ መደብ :- የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ባለሙያ
ደረጃ፡ VIII

ዋና ዋና ተግባርና ኃላፊነት	ዕውቀት	ክህሎት	የት/ደረጃ	ሥራ ልምድ	ሰርተፍኬት

➢ የተለያዩ ሞዴሎችን፣ ፖሊሲ፣ ስታንዳርዶችን፣ ወዘተ የመቅረፅ ብቃት (technical and managerial)	➢ የሳይበር ምህዳሩን ከተቋሙ አሁናዊ እንቅስቃሴዎችና የወደፊት እቅዶች ጋር በማስተሳሰር የሳይበር ጥቃቶችን መከላከል የሚያስችሉ ሞዴሎችንና ዲዛይኖችን መቅረፅ፤ ➢ ከተቋሙ አሁናዊ እንቅስቃሴዎችና የወደፊት እቅዶች ጋር የሚጣጣም የሳይበር ጥቃቶችን መከላከል የሚያስችልና የተቋሙን የሳይበር ደህንነት የሚያስጠብቁ ፖሊሲዎችን መቅረፅ፤ ➢ የቡድኑን የስራ ጥራት መለኪያ እና የስራ ግንኙነት መምሪያ ስታንዳርዶች ማዘጋጀት፤ ➢ ወጤታማና ወጪ ቆጣቢ የ Disaster recovery እቅድ ማዘጋጀት ፤
➢ Attackers tools, techniques, tactics and defense mechanisms	➢ ጥቃት አድራሾች የሚጠቀሙባቸውን የተለያዩ መሳሪያዎች፣ ዘዴዎች፣ መንገዶችና ለነዚህ የሚሆኑ ውጤታማ የመከላከያ መንገዶች እውቀት (በዓለም ላይ የሚታወቁና የራሱንም መፍጠር)፤
➢ መምራት እና ስልታዊ እቅዶችን የማውጣት አቅም፤	➢ የተቋሙን የሳይበር ደህንነት ክስተት አስተዳደር አጠቃላይ ስራ እና አተገባበር ስልታዊ (strategic) እቅድ ያዘጋጃል፣ ይመራል፤
➢ ምክረ ሃሳብ የማቅረብ ብቃት፤	➢ ተጨባጭ እና የተቋሙን ሁኔታ ባገናዘበ መልኩ ምክረ ሃሳብ ማቅረብ፤
➢ መሠነድ እና አቀራረብ፤	➢ አመታዊ ሪፖርቶችን በማዘጋጀት ለተቋሙ የበላይ አመራር ወይም ለሚመለከተው አካል የማቅረብ አቅም፤
➢ የመምራት አቅም፤	➢ እቅዶችን በተሳካ ሁኔታ ከማስፈፀምና ጥራት ያለው ወጤታማ ስራዎችን ከመስራት አንፃር የቡድን አባላትን ሰርቶ ማሰራት፣ ማብቃት፣ ግብረ መልስ በመቀበል ነገሮችን ማሻሻል፤

ክፍል አራት፡ የማዕቀፉ አተገባበር

4.1. ማዕቀፉን ከተቋማት አውድ ጋር ስለማጣጣም

የሳይበር ደህንነት አደረጃጀት እና የሥራ መደቦች ማዕቀፍ ከተቋማት አውድ አንጻር በማናበብ የሚተገበር ሲሆን እነዚህ ተቋማት በቴክኖሎጂ አጠቃቀማቸው በተለያየ ደረጃ ላይ የሚገኙ ናቸው። በመሆኑም አንዳንድ ተቋማት ሙሉ በሙሉ በኢንፎርሜሽን ቴክኖሎጂ ላይ ጥገኛ የሆኑና እያንዳንዱ የአገልግሎት አሰጣጣቸው በቴክኖሎጂ የታገዘ ሲሆን ሌሎቹ ደግሞ እምብዛም አይደሉም። ስለሆነም የተቋማትን ተልዕኮ፣ የሥራ ባህሪይ እንዲሁም አሁን ያሉበት የአቅም ደረጃ፣ ቀጣይ ዕድገት እና ሊደርሱ የሚችሉበትን የወደፊት አቅም ታሳቢ በማድረግ በዚህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ ውስጥ የተጠቀሱ አደረጃጀቶችን በሁሉም የመንግስትና ቁልፍ የግል ተቋማት ውስጥ ተግባራዊ እንዲሆን ከታች የተገለጸውን ተቋማዊ የብስለት(አቅም) ደረጃ መስፈርቶች መነሻ ተቋማት ከራሳቸው አውድና አቅም አንጻር ወስደው አደረጃጀቶቹን ተግባራዊ ያደርጋሉ።

የተቋማት የብስለት(አቅም) ደረጃ	መስፈርት	የሚተገበሩ አደረጃጀቶች
ደረጃ 4	➢ ተቋሙ ቁልፍ የመሰረተ ልማት ተቋማት ተብለው ከተለዩት ተቋማት ውስጥ የሚካተት ከሆነ፤ ➢ ተቋሙ የራሱ የኢንፎርሜሽን መሰረተ ልማቶችና ስርዓቶች ያለው ከሆነ፤	➢ ሳይበር ደህንነት ንቃተ ህሊና ➢ ሳይበር ደህንነት አስተዳደር ➢ ሳይበር ደህንነት ኢንጂነሪንግ ➢ ሳይበር ደህንነት ኦዲት እና ግምገማ ➢ ሳይበር ደህንነት ክስተት ክትትል እና ምላሽ
ደረጃ 3	➢ የተቋሙ አገልግሎት አሰጣጥ እና የመረጃ አያያዝ ሙሉ በሙሉ በሚባል ደረጃ በቴክሎጂ የተደገፈ ከሆነ፤ ➢ የተቋሙ ዋና ዋና የስራ ሂደት በኢንፎርሜሽን ቴክኖሎጂ የተደገፈ ከሆነ፤ ➢ የራሳቸው የኢንፎርሜሽን መሰረተ ልማት እና ኢንፎርሜሽን ስርዓት ባይኖራቸውም በሌሎች የሚጠቀሙ፤	➢ የሳይበር ደህንነት አስተዳደር ቡድን ➢ ሳይበር ደህንነት ንቃተ ህሊና ➢ ሳይበር ደህንነት ኢንጂነሪንግ

ደረጃ 2	➢ የተቋሙ አገልግሎት አሰጣጥ እና የመረጃ አያያዝ በከፊል በሚባል ደረጃ በቴክሎጂ የተደገፈ ከሆነ፤ ➢ የስራ ባህሪያቸው ድጋፍ እና ቁጥጥር ላይ ያደረጉ ተቋማት፤	➢ ሳይበር ደህንነት አስተዳደር
ደረጃ 1	➢ የተቋሙ አገልግሎት አሰጣጥ እና የመረጃ አያያዝ በቴክሎጂ ያልተደገፈ ከሆነ፤ ➢ የተደራጀ ተቋማዊ መረጃዎች የሌላቸው፤ ➢ ዋና ዋና የስራ ሂደታቸው በኢኮቴ ላይ ያልተመሰረተ ከሆነ፤ ➢ ዝቅተኛ የኢኮቴ መሰረተ ልማት ያላቸው፤ ➢ ዝቅተኛ የኢኮቴ መሰረተ ልማት የእርስ በእርስ ግንኙነት ያላቸው፤	➢ ምንም የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ወስደው ሊተገብሩ አይችሉም፤

4.2. በማዕቀፉ አተገባበር ወቅት ትኩረት የሚሰጣቸው ጉዳዮች

ሀ. ይህ የሳይበር ደህንነት አደረጃጀት በእያንዳንዱ ተቋም ከኢኮቴ የሥራ ክፍል በተለየ ሁኔታ ይደራጃል፤ ይቋቋማል፤

ለ. ይህንን ማዕቀፍ ተግባራዊ ለማድረግ በቅድሚያ ተቋማት የራሳቸውን አውድ በአግባቡ ማጤን ይኖርባቸዋል፤

ሐ ከላይ በተራ ቁጥር 4.2 ላይ የተገለጸው እንደተጠበቀ ሆኖ ተቋማት የራሳቸውን የአቅም (የብስለት) ደረጃ እና የተገለጸውን መስፈርት ከግምት ውስጥ በማስገባት አደረጃጀቶችንና የሥራ መደቦችን በሚገባ መለየት ይኖርባቸዋል፤

መ. ቁልፍ የግል ተቋማት ይህንን ማዕቀፍ የራሳቸውን አቅም በሚገባ በመለየት አስፈላጊነቱን ሲያምኑበት/ሲታመንበት/ ተግባራዊ ማድረግ ይችላሉ፤

4.3. ስለማዕቀፉ አተገባበር

4.3.1 በተራ ቁጥር 4.1. የተጠቀሰው እንደጠበቀ ሆኖ ይህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ በቁልፍ የኢንፎርሜሽን መሠረተ ልማት ተብለው በተለዩ ተቋማት ላይ ተግባራዊ ይሆናል፡፡

4.3.2 በተራ ቁጥር 4.1. የተጠቀሰው እንደተጠበቀ ሆኖ ከቁልፍ የኢንፎርሜሽን መሠረተ ልማት

ተቋማት ውጪ ያሉ የመንግስት ተቋማት ማዕቀፉን እንደየተቋማቸው አቅም እንዲሁም አውድ ታሳቢ በማድረግ በተጠቀሰው መስፈርት መሰረት ተግባራዊ ያደርጋሉ፡፡

4.3.3 የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ የማዕቀፉን አፈጻጸም የመቆጣጠር እና ድጋፍ የመስጠት ኃላፊነት ይኖረዋል፡፡

4.4. የማዕቀፉ አለመፈጸም የሚያስከትለው ተጠያቂነት

ሀ. ይህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ ምክንያታዊ ባልሆነ ሁኔታ አለመፈጸሙ ሲረጋገጥ ማዕቀፉ እንዳይፈጸም ባደረገው አካል ላይ አግባብ ባለው የመንግሥት አዋጅ፣ ደንብና የሲቪል ሰርቪስ የሥራ መመሪያዎች ወይም እንደየተቋማቱ የአሰራር መመሪያዎች መሠረት እና እንደየጥፋቱ ሁኔታ እየታየ ተጠያቂ ሊሆን ይችላል፡፡

ለ. በዚህ ማዕቀፍ የተቀመጡትን ተግባሮችና ሃላፊነቶች በማወቅ ወይም በቸልተኝነት ያልፈጸመ ማንኛውም ኃላፊና ሠራተኛ በፌዴራል የመንግሥት ሠራተኞች አዋጅ መሰረት የዲስፕሊን እርምጃ ይወሰድበታል፡፡ እንዲሁም እንደየተቋማቱ የዲሲፕሊን አፈጻጸም መመሪያ መሠረት ተጠያቂ ይሆናል፡፡

4.5. ማዕቀፉን ስለማሻሻል

ይህ የሳይበር ደህንነት አደረጃጀት እና የሥራ መደብ ማዕቀፍ በኢመደኤ ሲታመንበት ብቻ ሊሻሻል ይችላል፡፡

አባሪዎች

የሳይበር ደህንነት ዳይሬክቶሬት ዳይሬክተር (ዋና ክፍል ኃላፊ)

ዕውቀት	ክህሎት	የት/ደረጃ	ሰርተፍኬቶች
➢ የሳይበር ደህንነት ስትራቴጂ እና ስልት ቅየሳ፤ ➢ የሳይበር ደህንነት አስተዳደር እና አመራር ስርዓት ግንባታ እና ቀረፃ፤ ➢ የሳይበር ደህንነት ስጋቶችና ተጋላጭነቶች የመከታተል፣ መልስ የመስጠት እና የመምራት፤ ➢ አዳዲስ የሳይበር ደህንነት ስጋቶችን እና ተጋላጭነቶችን የመለየት እና ተገቢውን እርምት የመውሰድ፤ ➢ የሳይበር ደህንነት ሪፖርት የማዘጋጀት እና የማቅረብ፤ ➢ የሳይበር ደህንነት ፖሊሲዎች እና ፕሮሲጀር ውጤታማነት በየጊዜው የመፈተሽ፣ የመገምገም እና የማረጋገጥ፤ ➢ የሳይበር ደህንነት ስጋት፣ ተጋላጭነት እና አደጋ የጥናት እና የመተንተን፤	➢ የደህንነት መረጃ እና ክስተት አስተዳደር፤ ግጭት የመፍታት፤ ➢ የሳይበር ደህንነት የመቆጣጠርና የመምራት፤ ➢ የተቋሙ ወሳኝ ሀብቶች እና መሰረተ-ልማት ላይ የሚደረገውን የኢንፎርሜሽን ሪስክ አስተዳደር ፕሮግራም የማቀድ፣ የመምራት፣ የመገምገም፤ ➢ የመለየትና የመምረጥ፣ ውጤታማ እና አዋጭ የሆኑ ውጥኖችና መፍትሄዎች የመንደፍ ክህሎት፤ ➢ የደህንነት መፍትሄዎች (securiy controls) የመስጠት፤	➢ የመጀመሪያ ዲግሪ በኮምፒዩተር ሳይንስ፣ በኮምፒዩተር ኢንጂነሪንግ፣ ማናጅመንት ኢንፎርሜሽን ሲስተምስ፣በሳይበር ደህንነት ወይም ኢንፎርሜሽን ቴክኖሎጂ እና ተመሳሳይ የሙያ ዘርፍ ➢ ሁለተኛ ዲግሪ በሳይበር ደህንነት፣ በኮምፒዩተር ኢንጂነሪንግ፣ ማናጅመንት ኢንፎርሜሽን ሲስተምስ፣ ወይም ኮምፒተር ሳይንስ እና ተመሳሳይ የሙያ ዘርፍ	➢ CISM (Certified Information Security Manager) **ወይም** ➢ CISSP (Certified Information System Security Professional) **ወይም** ➢ CCISO (Certified Chief Information Security Officer) **ወይም** ➢ ISO Risk management **ወይም** ➢ Certified vulnerability assessor or CEH **ወይም** CCNAS, Cisco Certified Network ➢ Associate Security CCNPS Cisco **ወይም** ➢ Certified Information Systems Auditor (CISA) **ወይም** ➢ Certified Network Professional Security ቢኖረው/ራት ይመረጣል፤

ማሳሰቢያ፦ ተቋማት የሳይበር ደህንነት ዳይሬክቶሬት ዳሬክተር (ዋና ክፍል ኃላፊ) በሚመድቡበት ወቅት ይህንን ከላይ በቅጽ 1 የተቀመጠውን መስፈርት ታሳቢ ቢያደርጉ ይመረጣል።

ለሳይበር ደህንነት ዳይሬክቶሬት ዳይሬክተር (ዋና ክፍል ኃላፊ) የሚያስፈልጉ የመወዳደሪያ አቅሞች/Competency/

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የሥራ ከባቢ የመገንዘብ ብቃት፤	➢ የተቋሙን አውድ ባማከለ መልኩ የሳይበር ደህንነት አስተዳደር ስራዎች ለማከናወንና ጅምር ውጥኖችን ከግብ ለማድረስ የተቋሙን ራዕይ፣ ተልእኮ፣ መዋቅር፣ ግቦች፣ አላማዎች፤ እንዲሁም የተቋሙን የስራ ባህል፣ ፍልስፍና የስራ-ሂደቶች የማወቅ ብቃት፤ ➢ የሀገሪቱን ፖለቲካዊ ፣ ኢኮኖሚዊ፣ ማህበራዊና ህጋዊ ፍላጎቶችን የመረዳት ብቃት፤ ተቋማዊ፣ ሀገራዊና አለም-አቀፋዊ ትስስርን፣ አለም-አቀፍ ቴክኖሎጂያዊ አዝማሚያዎች እና ሌሎች አውዳዊ ጉዳዮችን የመገንዘብ ብቃት፤
➢ የአመራር ብቃት፤	➢ የሳይበር ደህንነት ሥራዎች ውጤታማ እንዲሆኑና የታለመላቸውን አላማ እንዲያሳኩ በተቀመጠላቸው መለኪያ፣ የጊዜ ገደብ እና በጀት መሰረት እንዲከናወኑ አስፈላጊ ቁሳቁሶች እንዲሟሉ የማድረግ፣ የግዜ ሰሌዳውን የመቅረፅ፣ የሚመለከታቸውን አካላት የማሳወቅ እና ስራዎችን በሚገባ እንዲሰሩ የመምራት፤ ➢ በአስተዳደራዊ ጉዳዮች ላይ ንቁ ተሳትፎ የማድረግ ብቃት፤
➢ የትንተና እና ችግሮችን የመፍታት ብቃት፤	➢ በተቋሙ ኢንፎርሜሽን እና ኢንፎርሜሽን ስርአተ-ሀብቶች ላይ የሚያጋጥሙና ያጋጠሙ ስጋቶችና አደጋዎች የሚያደርሱት ፖለቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊ ተፅእኖ እና የአደጋዎቹን ባህሪ ሁለንተናዊነት በተላበሰ አኳሃን የመቃኘት፣ የመገንዘብና የመተንተን፤ እንዲሁም መፍትሄዎችን የማስቀመጥ፣ የማስተሳሰር፣ አዋጭነታቸውን የማረጋገጥ ብቃት፤
➢ የንድፍ ብቃት፤	➢ የተቋሙን የሳይበር ደህንነት ስትራቴጂዎችን፣ ካሪኩለሞችን፣ ይዘቶችን፣ ማንዋሎችን፣ የተግባር ዕቅዶችን እና ዘዴዎችን የመንደፍ ብቃት፤
➢ የግምገማ ብቃት፤	➢ ተቋማዊ የሳይበር ደህንነት ባህሪና ለውጦችን የመገንዘብ፣ የመገምገም፣ የመመርመር፣ የተወሰዱ ትምህርቶችን የመሰነድ፣ ምክረ ኃሳቦችን እና ማስተካከያዎችን የማስቀመጥ ብቃት፤
➢ ተጽእኖ የመፍጠር ብቃት፤	➢ የተቋሙን አውድ ያማከሉ የሳይበር ደህንነት ፕሮግራሞች መቅረጽ እና አስፈላጊነታቸውን አግባብ ባለው ሁኔታ የማስረዳት፣ የማሳመን እና የሳይበር ደህንነት ስጋቶች ምን ያህል ተፅእኖ ማሳደር እንደሚችሉ የማስረዳት ብቃት፤ ➢ ስጋቶችን ለመቀነስ ወይም ለማስወገድ የተመረጡት ቴክኒካዊና አስተዳደራዊ መፍትሄዎች ተቀባይነት አግኝተው ተግባራዊ እንዲሆኑ አግባብ ባለው ሁኔታ ተጽእኖ የመፍጠር ብቃት፤
➢ የፈጠራ ብቃት፤	➢ ለተቋሙ አስፈላጊ እና ወቅታዊ የሆኑ የሳይበር ደህንነት ፕሮግራሞችን፣ ስርዓቶች (ሞዴሎች፣ ሜትዶሎጂዎች፣ ፍሬምዎርኮች፣ ጋይድላይኖች፣ ፕሮሲጀሮች ወዘተ) መቅረጽ፣ ማልማት፤ እንዲሁም በየጊዜው የመገምገም እና የማሻሻል ብቃት፤

➢ ከለውጥ ጋር የመራመድ ባህል፤	➢ ከሳይበር ደህንነት ጉለዋቁ ባህሪ ጋር ተያይዞ የሚመጡትን ለውጦች እንደ አስፈላጊነታቸው የጉቋመን ተልእኮና ራዕይ ማሳካት በሚያስችል መልኩ ተግባራዊ የማድረግ ባህል፤

ሳይበር ደህንነት መሪ ኮሚቴ (Steering) የመወዳደሪያ አቅሞች (competency)

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የተግባቦት ክህሎት፤	➢ በተቋም ውስጥ የሚከናወኑ የሳይበር ደህንነት ጉዳዮችን ከተለያዩ ክፍሎችና ከባለድርሻ አካላት ጋር በመግባባት የመስራት ብቃት፤
➢ በቡድን የመስራት /መረዳዳት/ ብቃት፤	➢ በተቋም ውስጥ የሚከናወኑ የሳይበር ደህንነት ጉዳዮችን ከተለያየ አካላት ጋር በጋራ እና በትብብር የመስራት ብቃት፤
➢ ፕሮጀክት የመምራት ብቃት፤ /ፕሮጀክት የመገምገም ብቃት/	➢ የሳይበር ደህንነት ፕሮጀክቶች ተቋሙ ላይ የሚያመጡትን ተጽዕኖ ከግምት ውስጥ በማስገባት የሳይበር ደህንነት ፕሮጀክቶችን የመምራት/ የመገምገም/ ብቃት፤
➢ የህግ እና ፖሊሲ የመገንዘብ ብቃት፤	➢ በሳይበር ደህንነት ህግ እና ፖሊሲ ስራዎችን በበላይነት መምራት እና የሚከናወኑት የሳይበር ደህንነት ስራዎች ከህግና ከፖሊሲ አንጻር ያላቸውን ተያያዥነት የማየት ብቃት፤

ማሳሰቢያ፡ በሳይበር ደህንነት መሪ ኮሚቴ ምደባ ወቅት በዚህ ቅጽ 3 የተቀመጠውን የመወዳደሪያ አቅም ታሳቢ ሊደረግ ይገባል።

የሳይበር ደህንነት አስተዳዳር ቡድን (ክፍል) መሪ የመወዳደሪያ አቅሞች/Competency/

የመወዳደሪያ አቅም	ማብራሪያ
➢ የመሰነድ ብቃት፤	➢ የሳይበር ደህንነት ገዢ ሰነዶች ለማዘጋጀት ውስብስብነት ያላቸው ሃሳቦች ማቀናጀት፣ ፍሰቱን በጠበቀ እና ግልፅ በሆነ መንገድ መሰነድ፤
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ በተቋም ደረጃ ተፅእኖ ያላቸው የሳይበር ደህንነት ገዢ ሰነዶች ተቀባይነት እንዲያገኙ የማሳመን እና ተጽእኖ የመፍጠር ብቃት፤
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ የተለያየ የስራ ባህል እና የስራ ከባቢ፣ ማህበራዊ እምነት፣ የትምህርት ድህረ-ታሪክ፣ የሙያ ድህረ-ታሪክ ያላቸው እና በተለያዩ እድሜ ክልል የሚገኙ ሰዎችን በሙያዊ ስነ-ምግባር፣ በጥንቃቄ፣ ውጤታማነትን በሚያሳናፅፍ መልኩ እና መልካም ስነ-ምግባር በተላበሰ አካኋን ተግባብቶ አብሮ ለመስራት የሚያስችል ብቃት፤
➢ የመፍጠርና የማሻሻል ብቃት፤	➢ በተቋም ደረጃ ተፅእኖ ሊፈጥሩ የሚችሉ የሳይበር ደህንነት ገዢ ሰነዶችን የማበልጸግ፣ የመፍጠር እና የማሻሻል ብቃት፤

ማሳሰቢያ፡- በሳይበር ደህንነት አስተዳደር ቡድን (ክፍል) መሪ ምደባ ወቅት የዕውቀት፣ የክህሎት፣ የት/ደረጃ፣ የሥራ ልምድና ስርተፍኬሽን በማዕቀፉ ክፍል ሶስት ለሳይበር ደህንነት አስተዳዳር የሥራ መደቦች የተቀመጠውን እንደ ዝቅተኛ መስፈርት አድርጎ መውሰድ ይቻላል።

የሳይበር ደህንነት ንቃተ ህሊና የሥራ ቡድን (ክፍል) መሪ የመወዳደሪያ አቅሞች /competencey/

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የመግባባት እና የመቀናጀት ብቃት፤	➢ የተለያየ የስራ ባህል እና የስራ ከባቢ፣ ማህበራዊ መስተጋብር፣ የትምህርት ድህረ-ታሪክ፣ የሙያ ድህረ-ታሪክ ያላቸው እና በተለያዩ እድሜ ክልል የሚገኙ ሰዎችን በሙያዊ ስነ-ምግባር፣ በጥንቃቄ፣ ውጤታማነትን በሚያሳናፅፍ መልኩ እና መልካም ስነ-ምግባር በተላበሰ አኳሀን ተግባብቶ እና አብሮ ለመስራት የሚያስችል ብቃት፣
➢ የመተንተን ብቃት፤	➢ በተቋም ደረጃ በወሳኝ ኢንፎርሜሽን እና ኢንፎርሜሽን ስርአት ሀብቶች ላይ ያጋጠሙ አደጋዎች የሚያደርሱት ተጨባጭ ፖለቲካዊ፣ ኢኮኖሚያዊ እና ማህበራዊ ተፅእኖዎች እና አደጋዎቹን ባህሪ ሁለንተናዊነት በተላበሰ አኳሃን የመቃኘት፣ የመገንዘብና የመተንተን ብቃት፣
➢ ተቋማዊ ንቃተ-ህሊና የማጎልበት ብቃት፤	➢ ወቅታዊ የሳይበር ደህንነት ሁኔታዎችን በመከታተል የተቋሙን አውድ መሰረት በማድረግ የሳይበር ደህንነት ንቃተ ህሊና ደረጃዎችን ለማሻሻል በተከታታይነት እና ቀጣይነት ባለው መልኩ ፕሮግራም ቀርጾ የሌሎች የተቋሙን አካላት ንቃተ-ህሊና ማጎልበት፤
➢ ለውጥ የማስተዳደር ብቃት፤	➢ ከሳይበር ደህንነት ጋር ተያያዥ የሆኑ ለውጦች በሚኖሩ እና በሚያጋጥሙ ጊዜ የተቋሙን አውድ መሰረት በማድረግ የመጡትን ለውጦች የማስተዳደር ብቃት፣
➢ የግንኙነት/ተግባቦት/ ብቃት፤	➢ የሳይበር ደህንነት ሁኔታን በተመለከተ መረጃውን ሊያውቁት ለሚገባቸው አካላት እንዲተላለፍ ማድረግ፣ ➢ የሳይበር ደህንነት ከሚመለከታቸው አካላት ጋር በሚኖሩ ውይይቶች እና ሌሎች ግንኙነቶች እራስን የመግለጽ ብቃት፣ ➢ በውይይቶች ወቅት ተጽእኖ ያላቸውን ተሳታፊዎች ለማሳመን የሚረዱ የቃል እና የጽሑፍ ግንኙነቶችን የማቀድ እና የማቅረብ ብቃት፣

ማሳሰቢያ፡- በንቃተ ህሊና ቡድን (ክፍል) መሪ ምደባ ወቅት የዕውቀት፣ የክህሎት፣ የት/ደረጃ፣ የሥራ ልምድና ስርተፍኬሽን በማዕቀፉ ክፍል ሶስት ለንቃተ ህሊና የሥራ መደቦች የተቀመጠውን እንደ ዝቅተኛ መስፈርት አድርጎ መውሰድ ይቻላል።

ቅጽ 6

የሳይበር ደህንነት ኢንጂነሪንግ የሥራ ቡድን (ክፍል) መሪ የመወዳደሪያ አቅሞች /Competency/

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የተፅእኖ ፈጣሪነት ብቃት፤	➢ የሳይበር ደህንነት ምህንድስና ስራዎች በተቋሙ ውስጥ በአግባቡ እንዲከናወኑ እና ተቀባይነት እንዲያገኙ የማሳመን እና ተጽእኖ የመፍጠር ብቃት፣
➢ የአመራር ብቃት፤	➢ የተቋሙ የሳይበር ደህንነት ምህንድስና ስራ አመራር ተቋሙ በሚያስቀምጣቸው ህጎች፣ መመሪያዎች፣ ፍልስፍናዎች እና ደንቦች መሰረት የመምራት ብቃት፤
➢ ፕሮጀክት ማስተዳደር፤	➢ የተቋሙን የሳይበር ደህንነት ምህንድስና ፕሮጀክት የሚያስፈልገውን ግብአትና አቅም በማስተባበር ደህንነትን ሊያረጋግጥ በሚችል መልኩ የማስተዳደር ብቃት፤
➢ አርክቴክቸር የመንደፍ ብቃት፤	➢ ማዕቀፎችን፣ አርክቴክቸር የመስሪያ ዘዴዎችን፣ እንዲሁም የሳይበር ደህንነት ስጋት ግምገማ ውጤትን እና የተመረጡ ቴክኖሎጂዎችን መሠረት በማድረግ የሳይበር ደህንነት አርክቴክቸር የማበልጸግ ብቃት፤
➢ ስታንዳርዶችን፣ ሞዴሎችን እና ማዕቀፎችን የመረዳትና የመተግበር ብቃት፤	➢ በዘርፉ በተለያዩ ዶሜኖች ሰፊና ጥልቅ ዕውቀት እንዲሁም የተፈተኑ ልምዶችን የያዙ አንዳንዴም እንድንጠቀማቸው የምንገደዳቸው ስታንዳርዶች፣ ሞዴሎች እና ማዕቀፎች ጠንቅቆ መረዳትና መተግበር መቻል፤
➢ የደህንነት ስጋት የመገምገም ብቃት፤	➢ የተለያዩ ስታንዳርዶችን፣ ዘዴዎችን እና መሳሪያዎችን በመጠቀም የደህንነት ስጋት ግምገማ መተግበርና የምላሽ ስትራቴጂ ማስቀመጥ፤
➢ ተጋላጭነት ፍተሻ ብቃት (vulnerability assessment)	➢ የተለያዩ ዘዴዎችን እና መሳሪያዎችን በመጠቀም የቴክኒካል ተጋላጭነት ፍተሻ መስራት እና ሪፖርት ማቀናበር መቻል፤
➢ የመረጃ ደህንነት የማረጋገጥ ብቃት፤	➢ ፖሊሲዎችን እና ፕሮሲጀሮችን በመረዳት እና በመከተል የመረጃን ተዓማኒነት፣ ሚስጢራዊነት እና ተደራሽነት የሚያረጋግጡ ቴክኒካል ኮንትሮሎች የመምረጥና የመትከል፤
➢ አፕሊኬሽን ደህንነት የማረጋገጥ ብቃት፤	➢ ፖሊሲዎችን እና ፕሮሲጀሮችን በመረዳት እና በመከተል የመረጃ ስርዓቶችን ከሚደርሱ ጥቃቶች ለመጠበቅ የሚረዱ ቴክኒካል ኮንትሮሎች የመምረጥና የመትከል፤

➢ ኔትዎርክ ደህንነት የማረጋገጥ ብቃት፤	➢ ፖሊሲዎችን እና ፕሮሲጀሮችን በመረዳት እና በመከተል የመረጃ ስርዓቶችን እና የኔትወርክ አገልግሎቶችን ከሚደርሱ ጥቃቶች ለመጠበቅ የሚረዱ ቴክኒካል ኮንትሮሎች የመምረጥና የመትከል፤
➢ System harden የማድረግ ብቃት፤	➢ የሲስተም ተጋላጭነትን በመለየት እና የpatch managment እንዲሁም የconfiguration አስተዳደር ሂደትን በመከተል የሲስተም ማጠንከር ሥራ የመሥራት፤
➢ የኔትዎርክ እና ደህንነት ቴክኖሎጂዎችን የመትከል እና የመፈተሽ ብቃት፤	➢ የደህንነት ስጋትን የሚቀንሱ ቴክኖሎጂዎችን በጥልቀት በመረዳት እና ደረጃውን የጠበቀ የተከላና የፍተሻ ሥራ የማከናወን ብቃት፤

ማሳሰቢያ፡- በኢንጂነሪንግ ቡድን (ክፍል) መሪ ምደባ ወቅት የዕውቀት፣ የክህሎት፣ የት/ደረጃ፣ የሥራ ልምድና ስርተፍኬሽን በማዕቀፉ ክፍል ሶስት ለኢንጂነሪንግ የሥራ መደቦች የተቀመጠውን እንደ ዝቅተኛ መስፈርት አድርጎ መውሰድ ይቻላል።

ቅጽ 7

የሳይበር ደህንነት ኦዲት እና ግምገማ ቡድን (ክፍል) መሪ የመወዳደሪያ አቅሞች (Competency)

የመወዳደሪያ አቅሞች	ማብራሪያ
➢ የጥራት ማረጋገጥ (Quality Assurance) ፤	➢ ሙከራው እንደተጠበቀው ስለመሆኑ ማረጋገጫ መስጠት፤
➢ የሙከራ አስተዳደር (Test Management) ፤	➢ እቅድ ማውጣት ፣ የሚፈለገውን ሃብት መመደብ እና ሙከራውን ማስተዳደር (Planning, allocating the resource required, and managing the test) ፤
➢ መረጃ የማደራጀት ብቃት፤	➢ የሳይበር ደህንነት ቁጥጥር እና ግምገማ በተመለከተ የተዘጋጁ ማኑዋል፣ ሪፖርት፤ መፈተሻ ዝርዝር (checklist) እና ሌሎች ተያያዥነት ያላቸው ሰነዶች በጥንቃቄ የመከፋፈል፣ የመጠበቅ እና የማደራጀት ብቃት፤
➢ ተጋላጭነትን የመለየት ብቃት፤	➢ በተቋሙ ላይ ሊኖሩ የሚችሉ ቴክኒካዊና አስተዳደራዊ ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ፈጣሪዎች፣ የስጋት አይነቶች የመለየትና የመገምገም ብቃት፤
➢ ችግሮችንና መፍትሄዎችን የማስተሳሰር ብቃት፤	➢ የተመረጡት የሳይበር ደህንነት መፍትሄዎች የተለዩ የሳይበር ደህንነት ስጋቶችን ምን ያክል መቅረፍ እንደሚችሉና አዋጭነታቸውን የማረጋገጥ ብቃት፤
➢ ተጋላጭነት የመለየት እና የግምገማ ብቃት፤	➢ የተቋሙን ወሳኝ የመረጃ ስርዓቶች፣ መረጃዎች እና መሰረተ-ልማቶች ኢላማ ለመፈተሽ፣ የሚያገለግሉ የኢላማውን ደካማ ጎኖች የመለየት የመገምገም፤ ➢ በተቋሙ ላይ ሊኖሩ የሚችሉ ቴክኒካዊና አስተዳደራዊ ክፍተቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት ፈጣሪዎች፣ የስጋት አይነቶች የመለየትና የመገምገም ብቃት፤
➢ Functional and non-functional testing(ሙከራ)	➢ የስርዓት ጫና፣ ውጥረት፣ የአፈፃፀም ሙከራን እና ኢላማውን በሚመለከት ተቋሙን መደገፍ መቻል Functional and non-functional testing(ሙከራዎች) ግዴታዎች መለየት እና ሙከራ ማከናወን፤
➢ የፍተሻ እና ትንተና (Testing and Analysis Skills) ብቃት፤	➢ የሳይበር ደህንነት ኦዲትና ግምገማ ለማካሄድ የሚጠቅሙ የፍተሻ ስልቶችን የመረዳት እና የመተግበር ብቃት ፤ እንዲሁም በየኦዲትና ግምገማ ሂደት ውስጥ የተገኙትን ውጤቶች የመተንተን ብቃት፤
➢ ህጎችንና ደንቦችን የመረዳት ብቃት፤	➢ የሳይበር ደህንነት ኦዲትና ግምገማ ስራዎች በሚከናወኑበት ወቅት ተያያዥነት ያላቸው የሳይበር ደህንነት ህጎችና ደንቦችን መሰረት በማድረግ የመስራት እና የመረዳት ብቃት፤

ማሳሰቢያ፡- በሳይበር ደህንነት ኦዲት እና ግምገማ ቡድን (ክፍል) መሪ ምደባ ወቅት የዕውቀት፣ የክህሎት፣ የት/ደረጃ፣ የሥራ ልምድና ሰርተፍኬሽን በማዕቀፉ ክፍል ሶስት ለኦዲት እና ግምገማ የሥራ መደቦች የተቀመጠውን እንደ ዝቅተኛ መስፈርት አድርጎ መውሰድ ይቻላል፡፡

ቅጽ 8

የሳይበር ደህንነት ክስተት ክትትል እና ምላሽ ቡድን (ክፍል) መሪ የመወዳደሪያ አቅሞች /Competency/

የመወዳደሪያ አቅም	ማብራሪያ
➢ ከሁኔታዎች ጋር የመጣጣም ብቃት፤	➢ የሳይበር ደህንነት ክስተቶችን ለመቆጣጠር እና ለመከታተል ካለው ነባራዊ ሁኔታ ጋር ተናብቦ እና ተጣጥሞ (adaptable) የመስራት ብቃት፤
➢ የመተንተን ብቃት፤	➢ በተቋም ደረጃ በወሳኝ ኢንፎርሜሽን እና ኢንፎርሜሽን ስርአት ሀብቶች ላይ ያጋጠሙ ክስተቶችን፣ የሚያደርሱት ተጫባጭ ፖለቲካዊ፣ ኢኮኖሚያዊ፣ ማህበራዊ ተፅእኖ እና የአደጋዎቹን ባህሪ ሁለንተናዊነት በተላበሰ አኳሃን የመቃኘት፣ የመገንዘብና የመተንተን ብቃት፤
➢ የመፍጠርና የማሻሻል ብቃት፤	➢ የሳይበር ደህንነት ክስተት አስተዳደር ሂደቶችን የማዘጋጀት፣ የማበልጸግ፣ የመፍጠር እና የማሻሻል ብቃት፤
➢ የመግባባት እና የመቀናጀት ብቃት	➢ ከኢትዮ-ሰርት እና ከሌሎች የስራ ክፍሎች ጋር በሳይበር ደህንነት ክስተት አስተዳደር ዙሪያ የተቋሙን ራዕይ ማሳካት በሚያስችል መልኩ ተግባብቶና ተቀናጅቶ የመስራት ብቃት፤
➢ መረጃ የመሰብሰብ ብቃት፤	➢ በቅርበትና በርቀት (local and remote) በሚገኙ የመረጃ ስርዓት ላይ ያሉ ተጋላጭነቶችን ለመለየት የሚረዱ የተለያዩ መረጃዎችን (ምሳሌ ኦፐሬቲንግ ሲስተም፣ ሰርቪስ፣ የተከፈቱ ፖርቶች፣ ወዘተ) የመሰብሰብ ብቃት፤
➢ ለሳይበር ጥቃት ምላሽ የመስጠት ብቃት	➢ ሳይበር ደህንነት ክትትል እና ምላሽ (response) የሚደረግባቸው የሥራ ምህዳር የመለየት፣ቴክኖሎጂ የመጠቀም ታክቲካል እና ቴክኒካል ብቃት፤
➢ የግምገማ ብቃት (Evaluation)፤	➢ በተቋሙ የሳይበር ደህንነት ክስተት ቁጥጥርና ምላሽ ዙሪያ ያሉ ለውጦችን (ደረጃ፣ ባህልና ባህሪ) የመገንዘብ፣ የመገምገም፣ የመመርመር፣ የተወሰዱ ትምህርቶችን የመሰነድ፣ ምክረ ኃሳቦችን እና ማስተካከያዎችን የማስቀመጥ ብቃት፤
➢ ተጋላጭነትን የመለየት ብቃት፤	➢ በተቋሙ ኢንፎርሜሽንና ኢንፎርሜሽን ስርአት ሀብቶች ላይ ሊኖሩ የሚችሉ ቴክኒካዊ ክፍቶቶች፣ ስጋቶች፣ የስጋት ምንጮች፣ የስጋት አካላትና ፍላጎታቸው፣ የስጋት አይነቶች የመለየትና የመገምገም ብቃት፤
➢ የመሰነድ ብቃት	➢ በተቋም ደረጃ የሚያጋጥሙ ማናቸውንም የሳይበር ደህንነት ክስተቶች የመሰነድና ለሚመለከተው አካል የማቅረብ ብቃት፤

+251-11-371-71-14
Fax: +251-11-3-20-40-37
P.O.BOX: 124498
contact@insa.gov.et
www.facebook.com/INSA.ETHIOPIA
www.insa.gov.et
Addis Ababa
Ethiopia