

የሰው ኃይል ፕሮግራም ግለዊነት

በግል ሊላይ የሚችል መረጃ

SDWORKS

የማህበራዊ ዋስትና ቁጥሮች

የመረጃ ልቀት

የሰው ኃይል እና ስራ መምሪያ (DLR) ሰራተኞች የሥራቸውን ተግባራት ለማከናወን ሚስጥራዊ መረጃዎችን ሊቀበሉ ወይም ሊያስተናግዱ ይችላሉ። ይህ መምሪያ ሚስጥራዊ መረጃዎችን አያያዝን ያካትታል። ይህም ደንበኛ ስለሆኑታቸው ከ DLR ሰራተኞች ጋር የሚያካፍላቸውን የግል መረጃዎች እና በ DLR አገልግሎቶች አጠቃቀም ወቅት ከ DLR ሰራተኞች ወይም SDWORKS ስርዓት የተሰበሰበውን በግል ሊላይ የሚችል መረጃ (PII) ያካትታል። DLR ሰራተኞች ሚስጥራዊ መረጃዎችን እና የውህብ ደህንነትን በተመለከተ አመታዊ ስልጠና እንዲሰጡ ይጠበቅባቸዋል። DLR አስፈላጊ ሆኖ ሲገኝ ይህንን መምሪያ ሊያሻሽል ይችላል።

በግል ሊላይ የሚችል መረጃ

በተጠበቁ PII እና ስራ ባልሆኑ PII መካከል ያለው ልዩነት በዋናነት የተመሰረተው PII ከመውጣቱ የሚመጣውን "የጉዳት አደጋ" በተመለከተ በተደረገ ትንተና ላይ ነው።

1. የተጠበቁ PII - ከተገለጹ ስሙ ወይም ማንነቱ ከመረጃው ጋር የተገናኘ ግለሰብ ላይ ጉዳት ሊያስከትል የሚችል መረጃ። የተጠበቁ የPII ምሳሌዎች የማህበራዊ ዋስትና ቁጥሮች (SSNs)፣ የክሬዲት ካርድ ቁጥሮች እና የባንክ ሂሳብ ቁጥሮች ያሉ የፋይናንስ መረጃዎችን፣ የግል መረጃ፣ የቤት ስልክ ቁጥሮች፣ ዕድሜዎች፣ የልደት ቀናት፣ የጋብቻ ሁኔታ፣ የትዳር ጓደኛ ስሞች፣ የባዮሜትሪክ መለያዎች (የጣት አሻራዎች፣ የአይሪስ ቅኝቶች፣ ወዘተ)፣ የጤና መዝገቦች፣ የሕክምና ታሪክ፣ GED መዝገቦችን ጨምሮ የትምህርት መዝገቦችን እና የኮምፒውተር የይለፍ ቃላትን ያካትታሉ። ነገር ግን በእነዚህ ብቻ የተወሰኑ አይደሉም።
2. ስሜታዊ ያልሆነ PII - ቢገለጽም በራሱ የግል ጉዳት ሊያስከትል የማይችል መረጃ። በመሠረቱ፣ ከማንኛውም የተጠበቁ ወይም ያልተጠበቁ PII ጋር ያልተያያዘ ወይም በቅርብ ያልተያያዘ ራሱን የቻለ መረጃ ነው። ለምሳሌ የመጀመሪያ እና የአባት ስሞችን፣ የኢሜይል አድራሻዎችን፣ የንግድ አድራሻዎችን፣ የንግድ ስልክ ቁጥሮችን፣ የአጠቃላይ ትምህርት ማስረጃዎችን፣ ጾታ ወይም ዘር ያካትታሉ። ሆኖም ግን፣ እንደ ሁኔታው፣ የእነዚህ ነገሮች ጥምረት የተጠበቁ ወይም ስሜታዊ PII ተብሎ ሊመደብ ይችላል።

በ DLR የተሰበሰበው መረጃ ስሞችን፣ አድራሻዎችን፣ የስልክ ቁጥሮችን፣ ዜግነትን፣ ጾታ፣ ዘር፣ የማህበራዊ ዋስትና ቁጥርን፣ የፌዴራል የአሠሪ መለያ ቁጥርን፣ የክልል የአሠሪ መለያ ቁጥርን፣ ዕድሜን፣ የስራ ታሪክ፣ የትምህርት ውጤቶችን፣ የግለሰብን ፕሮግራም እና የአገልግሎት ብቁነት፣ ለፕሮግራሙ መዝገብ እና ለፕሮግራም ሪፖርት እና አፈጻጸም አስፈላጊ የሆኑ መረጃዎችን ያካትታል። ነገር ግን በእነዚህ ብቻ የተወሰኑ አይደሉም።

የ PII አያያዝ

የአሜሪካ የሰው ኃይል እና ስራ መምሪያ (ETA) ለ PII አያያዝ የሚከተሉትን መስፈርቶች አውጥቷል

1. ሰራተኞች ከደንበኞች ጋር ሙያዊ ወሰኖችን መጠበቅ እና ከድርጅቱ ውጭ ካሉ ግለሰቦች ጋር የደንበኛ መረጃን ከመወያየት መቆጠብ አለባቸው።
2. የደንበኛ መረጃ በሚከተሉት ምክንያቶች ብቻ ሊጋራ ይችላል፡
 - o ፕሮግራሞች አዳዳዮች ፤
 - o አስፈላጊ የፕሮግራም ሪፖርት ማድረግ፤
 - o በሙግት፣ በወንጀል ምርመራ ወይም በሌሎች የህግ ሂደቶች ወቅት የሚፈለጉ መግለጫዎች ፤ ወይም ከሌሎች የክልል ወይም የፌዴራል ኤጀንሲዎች ጋር የመረጃ መጋራት ስምምነቶች፤
 - o በደንበኛው የተፈረመ የመረጃ ልቀት በኩል በጽሑፍ ፈቃድ፤
 - o በደንበኛው የጽሑፍ ፈቃድ፣ በውህብ መጋራት ስምምነት ወይም እንደ ሪፖርት ማድረግ ወይም የፕሮግራም አዲት ላሉ የክልል ወይም የፌዴራል የፕሮግራም ዓላማዎች።

- o የደንበኛ መረጃ ለማግኘት የሚቀርቡ ህጋዊ ጥያቄዎች ለዲኤልኦር መዝገብ ጥያቄ ኃላፊ እና ለዲቪዥን ዳይሬክተር መቅረብ አለባቸው።
 - o GED® የትምህርት መዝገቦችን የሚጠይቁ ደንበኞች ወደ SD የትምህርት ክፍል GED® አስተዳዳሪ ሊመሩ ይችላሉ።
3. ለሁሉም የኤሌክትሮኒክስ ስርዓቶች ጠንካራ እና ልዩ የሆኑ የይለፍ ቃላት ጥቅም ላይ ይውላሉ። የይለፍ ቃላት እና የደህንነት ምስክርነቶች አይገቡም። አንድ ሰራተኛ ከስራ ሲወጣ ከምጥውተሮች መቆለፍ አለባቸው፤ ሌሎች የኮምፒውተር ስክሪኖችን ማየት እንዳይችሉ ጥንቃቄ ማድረግ ያስፈልጋል።
 4. መረጃው የመዝገቦችን/ሰነዶችን ሚስጥራዊነት ለመጠበቅ በሚያስችል መንገድ መከናወን አለበት እና ያልተፈቀደላቸው ሰዎች እንደዚህ አይነት መዝገቦችን እንዳያገኙ ለመከላከል የተነደፈ ነው። የPII መረጃ በማንኛውም ጊዜ ያልተፈቀደላቸው ሰዎች በአካል እንዳይደርሱበት ደህንነቱ በተጠበቀ ቦታ መቀመጥ አለበት ።
 5. ኢሜይል ወይም በተከማቹ ሲዲዎች፣ ዲቪዲዎች፣ አውራ ጣት ድራይቮች፣ ወዘተ የሚተላለፉ ሁሉም PII እና ሌሎች ሚስጥራዊ መረጃዎች የፌዴራል የመረጃ ማቀነባበሪያ ደረጃዎች (FIPS) 140-2 ተገዢ እና ብሔራዊ የደረጃዎች እና ቴክኖሎጂ ተቋም (NIST) የተረጋገጠ የክሪፕቶግራፊክ ሞጁል በመጠቀም መመስጠር አለባቸው። ክላሲክ እና ኒው አውትሉክ ኢሜይል ወይ ውጭ አካል ለማመስጠር አማራጭ ይሰጣሉ፣ ማለትም በstate.sd.us ጎራ ውስጥ አይደለም፣ ኢሜይል አማራጭ አዝራሩን በመጠቀም እና PII ከስቴት ስርዓቱ ውጭ ለመላክ 'Encrypt' የሚለውን በመምረጥ። PII እንደ ማይክሮሶፍት ፎርም እና አዶቤ ምልክት ባሉ ደህንነታቸው በተጠበቁ ዘዴዎች ሊተላለፍ ይችላል።
 6. እንደ SharePoint folders፣ SDWORKS ወይም LACES ያሉ ለተፈቀደላቸው PII ማከማቻ የተመደቡ ስርዓቶች ብቻ PIIን ለማከማቻ ሊያገለግሉ ይችላሉ። በግል ባለቤትነት በተያዙ መሰሪያዎች ላይ የETA መስጠት PII መረጃን ማግኘት፣ ማቀናበር እና ማከማቻ የተከለከለ ነው። የወረቀት ሰነዶች አይመከሩም፣ ነገር ግን አስፈላጊ በሚሆንበት ጊዜ በተቆለፈ ካቢኔ ውስጥ መቀመጥ አለባቸው እና እንደ መቆራረጥ ያሉ ተገቢ የማጥፋት ዘዴዎች ያስፈልጋሉ።
 7. መረጃው በፕሮግራሞቹ ከሚያስፈልጉት ውጪ ለሌላ ለማንኛውም ዓላማ ሊገኝ ወይም ጥቅም ላይ ሊውል አይችልም። የመረጃ ተደራሽነት የሚገደበው ስራ ወሰን ጋር በተያያዘ ሥራቸውን ለመወጣት በይፋዊ አቅማቸው ለሚፈልጉ ሰዎች ብቻ ነው።
 8. አካላዊ ሰነዶች እንደ መቆራረጥ ባሉ ሚስጥራዊነትን በሚጠብቅ ደህንነቱ በተጠበቀ መንገድ መጣል አለባቸው።
 9. ማንኛውም የተጠረጠረ የደህንነት ጥሰቶች ወይም ያልተፈቀደ መዳረሻ ወዲያውኑ ለቀጥታ ሱፐርቫይዘር እና ለዲቪዥን ዳይሬክተር መጋራት አለበት።
 10. ሚስጥራዊ መረጃ ወደ ያልተፈቀዱ የትርጉም አገልግሎቶች፣ የኢንተርኔት ፍለጋ ፕሮግራሞች ወይም አርቲፊሻል ኢንተላጀንስ ድረ-ገጾች መቅረብ የለበትም።

[ወደ ይዘቱ ማውጫ ተመለስ](#)

SDWORKS

የ SDWORKS ድህረ ገጽ ሥራ ፈላጊዎች፣ አሠሪዎች እና አጠቃላይ ሕዝቡ የሠራተኛ ልውውጥ ተግባራትን እንዲጠቀሙ እና ስለ ደቡብ ዳኮታ የሥራ ገበያ መረጃ እንዲያገኙ ያስችላቸዋል። SDWORKS በመለያ ምዝገባ ወቅት፣ SDWORKS በሚጠቀሙበት ጊዜ እና ድህረ ገጹን በሚጠቀሙበት ጊዜ የግል መረጃ በሚጠየቅበት ጊዜ ሁሉ PII ይሰበስባል። ይህ መረጃ የሚሰበስበው የፕሮግራም ታማኝነትን እና የወደፊት ማሻሻያዎችን ለማረጋገጥ የሰው ሃይል ሪፖርት ማድረግን እና የፕሮግራም አፈጻጸም መስፈርቶችን ለማሟላት ነው። በተጨማሪም፣ መረጃ በ SDWORKS ሊፈለጉ በሚችሉ የውሂብ ጎታ አገልጋዮች ውስጥ ለመለጠፍ የግል መገለጫ ወይም የስራ ዝርዝር ለመፍጠር ጥቅም ላይ ይውላል።

SDWORKS ተጠቃሚዎች በመስመር ላይ ለማስቀመጥ የኤሌክትሮኒክ የሥራ ዝርዝር ወይም የሥራ ዝርዝር መፍጠር ይችላሉ። በአካውንት ቅንብሮች ውስጥ፣ የተመዘገቡ SDWORKS ተጠቃሚዎች ሪቪው በአሠሪዎች ለሕዝብ እይታ ክፍት እንዲሆን የማድረግ አማራጭ አላቸው፣ ይህም እንደ አድራሻ፣ ስልክ፣ ኢሜይል፣ ወዘተ ያሉ በሪቪው ውስጥ ያሉ ማናቸውንም መረጃዎች ያካትታል። መረጃ ወደ ቀጣሪ ወይም ቀጣሪ ሲላክ፣ DLR ቀጣሪ ወይም የቀጣሪውን ማቆየት ፣ የመጠቀም ወይም የግላዊነት ልምዶችን የማስተዳደር ኃላፊነት የለበትም። PII፣ የተጠቃሚ ስሞች፣ የኢሜይል አድራሻዎች ወይም መልዕክቶች ከ SDWORKS በፈቃደኝነት ይፋ ማድረግ ከሌሎች ግለሰቦች ወይም ከሰበስቦች ወገኖች ያልተጠየቁ መልዕክቶችን ሊያስከትል ይችላል። እንደዚህ ያሉ እንቅስቃሴዎች ከ SDWORKS ስርዓት እና DLR ቁጥጥር ውጭ ናቸው።

አንድ ተጠቃሚ SDWORKS ድህረ ገጽን ሲጎበኝ የአይፒ አድራሻዎች እና የድር ጣቢያ አጠቃቀም መረጃ በራስ-ሰር ይሰበሰባል። ይህ መረጃ የጎብኚዎችን ባህሪ በአጠቃላይ ለመገምገም ይረዳል፤ ይህም የእያንዳንዱን ገጽ ጎብኚዎች ብዛት እና ድግግሞሽ እና እያንዳንዱ ገጽ የሚታየውን የጊዜ ርዝመት ያካትታል።

ኩባዎች ወደ ተጠቃሚ ኮምፒውተር ሊተላለፉ ይችላሉ። ኩባዎች የድር አሳሽ በኮምፒውተር ሃርድ ድራይቭ ላይ ወይም በኢንተርኔት ማሰስ ወቅት በኮምፒውተር ማህደረ ትውስታ ውስጥ የሚያስቀምጠው የመረጃ ፋይሎች ናቸው። ኩባዎች የተጠቃሚ ፋይሎችን ሊጎዱ ወይም ከሃርድ ድራይቭ መረጃን ማንበብ አይችሉም። SDWORKS ኩባዎች የተጠቃሚውን ክፍለ ጊዜ በድር ጣቢያው ውስጥ ባሉ ገጾች ውስጥ ሲያልፉ ለማቆየት ያገለግላሉ። SDWORKS ገጹን የተጠቃሚውን ፍላጎት በተሻለ ሁኔታ ለማሟላት የሚያበጅ መለያ ኩባን ያዘጋጃል።

የ SDWORKS ተጠቃሚዎች የኢሜይል አድራሻዎች፣ በተለይም ከክልል ውጭ ያሉ ነዋሪዎች፣ ለገበያ ጥናትና ማዳረስ ዓላማ ሊያገለግሉ ይችላሉ። እንዲሁ ዓይነቱ መረጃ እንደ Dakota Roots ያሉ የሰራተኞች ምልመላ ፕሮግራሞችን ጥረት ይደግፋል። ይህ ያልተጠየቀ ቀጥተኛ ደብዳቤ፣ ኢሜይል ፍንዳታ፣ ወዘተ ሊያስከትል ይችላል።

የድረ-ገጽ ጉብኝቶች፣ በድረ-ገጽ ላይ የሚያሳልፉት ጊዜ፣ ወደ የስራ ቅደም ተከተል የሚደረጉ ጉብኝቶች እና የሥራ ፍለጋዎች ስለ ደንበኞች አጠቃቀም እና የድረ-ገጽ አፈጻጸም የበለጠ ለማወቅ ይሰበሰባሉ።

አጠቃላይ መረጃው ለሶስተኛ ወገኖች ሊሰጥ የሚችለው DLR የሰው ሃይል ልማት ጥረቶችን ለማሻሻል እንዲረዳ ነው። የSDWORKS የስህተት ምዝግብ ማስታወሻ ስርዓት ቴክኒካል ሰራተኞቻችን ስህተቱን እንዲረዱ ለማገዝ ከማንኛውም SDWORKS ጣቢያ ስህተቶች ጋር የተያያዙ የተጠቃሚ ስሞችን ይሰበስባል።

የ SDWORKS ድህረ ገጽ ተጠቃሚን ወደ ሌሎች ድረ-ገጾች ለማሰስ የሚያስችሉ አገናኞችን ያቀርባል፤ እነዚህም የራሳቸው የመረጃ አሰባሰብ ልምዶች፣ የግላዊነት ፖሊሲዎች እና የደህንነት እርምጃዎች ሊኖራቸው ይችላሉ። ከ SDWORKS ወደ ሌሎች ድረ-ገጾች የሚሄዱ ጎብኚዎች የእነዚያ ድረ-ገጾች የግላዊነት ፖሊሲዎችን እና የመረጃ አሰባሰብ ልምዶችን ግምገማ አለባቸው።

እንደ SDWORKS ያሉ የአስተዳደር መረጃ ስርዓቶች፣ በተመደቡ ሰራተኞች ፈቃድ እና ለተፈቀደላቸው ዓላማዎች ብቻ ጥቅም ላይ ሊውሉ የሚችሉ ሚስጥራዊ መረጃዎችን ይይዛሉ። የሚገኙ የPII ስክሪኖች በማንኛውም ባልተፈቀደ መንገድ ሊታተሙ፣ ሊባዙ ወይም ሊሰራጩ አይችሉም።

SDWORKS መዳረሻ

የ SDWORKS ስርዓትን ደህንነት እና ታማኝነት ለማረጋገጥ የሚከተሉት እርምጃዎች ተግባራዊ ይሆናሉ

- **አካላዊ ደህንነት** : የውሂብ ጎታ አገልጋዮችን መድረስ ለተፈቀደላቸው ሰዎች ብቻ የተገደበ ነው።
- **የኤሌክትሮኒክ ደህንነት** :- መረጃው ያልተፈቀደ መጥለፍን ለመከላከል እና ደህንነቱ የተጠበቀ ግንኙነትን ለማረጋገጥ በኤስኤስኤል ምስጢራ የተጠበቀ ነው።
- **የግለሰብ መለያ ጥበቃ** : እያንዳንዱ ተጠቃሚ SDWORKS መለያውን ለመድረስ የራሱን የይለፍ ቃል መጠቀም አለበት። የይለፍ ቃሎች በፍፁም መጋራት የለባቸውም።
- **የክፍለ ጊዜ ደህንነት** : ተጠቃሚዎች ያልተፈቀደ መዳረሻን ለመከላከል ከእያንዳንዱ ክፍለ ጊዜ በኋላ የድር አሳሹን ዘግተው መዝጋት አለባቸው።
- **የውሂብ አጠቃቀም ገደቦች** : በስርዓቱ በኩል የሚደረስ መረጃ ከተፈቀደላቸው ፕሮግራሞች ጋር በቀጥታ ለተያያዙ ዓላማዎች ብቻ ጥቅም ላይ ሊውል ይችላል። ያለፍቃድ የውሂብ አጠቃቀም ወይም ስርጭት በጥብቅ የተከለከለ ነው። የPII ያላቸው SDWORKS ስክሪኖች መታተም፣ መባዛት ወይም መሰራጨት የለባቸውም።

[ወደ ይዘቱ ማውጫ ተመለስ](#)

የማህበራዊ ዋስትና ቁጥሮች

ሁሉም DLR ሰራተኞች የስራ ፈላጊዎችን እና የሌሎች ግለሰቦችን የማህበራዊ ዋስትና ቁጥሮች (SSNs) ደህንነት ለመጠበቅ ኃላፊነት አለባቸው።

DLR) ሕጋዊ ፈቃድ ለሌላቸው ሰዎች ወይም አካላት የማህበራዊ ዋስትና ቁጥሮችን (SSNs) ይፋ ማድረግን ይከለክላል። DLR ሰራተኞች የ2004ቱን የማህበራዊ ዋስትና ጥበቃ ህግ ወይም የ1974ቱን የግላዊነት ህግ በሚጠራው መልኩ የማንኛውንም ሰራተኛ ፣ ተማሪ ወይም ሌላ ግለሰብ የማህበራዊ ዋስትና ቁጥር (SSN) ሆን ብለው አያሳይም፣ አያጋልጥም፣ አያስተላልፍም ወይም ህገወጥ በሆነ ማንገድ አይጠቀሙም።

የማህበራዊ ዋስትና ቁጥር (SSNs) መሰብሰብ ያለበት በፌዴራል ወይም የመንግስት ህግ በሚጠየቅበት ጊዜ ብቻ ነው። ልዩ የግል መለያ የሚያስፈልግ ከሆነ፣ የማህበራዊ ዋስትና ቁጥር ምትክ በእሱ ቦታ ጥቅም ላይ ይውላል።

የማህበራዊ ዋስትና ቁጥር (SSNs) የሚያሳዩ ሰነዶች፣ ቁሳቁሶች ወይም የኮምፒውተር ስክሪኖች ሁልጊዜ ከሕዝብ እይታ ውጭ መሆን አለባቸው ።

የማህበራዊ ዋስትና ቁጥር (SSNs) የያዙ ሰነዶች የሚላኩት በክልል እና በፌዴራል ህግ ሲፈቀድ ብቻ ነው። የማህበራዊ ዋስትና ቁጥር (SSN) በግልጽ በተላከ ሰነድ ውስጥ ሊካተት ይችላል፤ እነዚህ ሁኔታዎች የሚከተሉትን ያካትታሉ፡

- ግለሰቡ የጀመረ ማመልከቻ ወይም የምዝገባ ሂደት አካል ሆኖ ይላካል።
- የተላከው አካውንት፣ ውል፣ ሰራተኛ ወይም የጤና መድን ጥቅማጥቅምን ለማረጋገጥ፣ ሁኔታውን ለማረጋገጥ፣ አገልግሎት ለመስጠት፣ ለማሻሻል ወይም ማቋረጥ - ወይም አካውንት፣ ውል፣ መመሪያ ወይም ሰራተኛ ወይም የጤና መድን ጥቅም ያለው ግለሰብ የማህበራዊ ዋስትና ቁጥር ትክክለኛነት ጥቅም ነው።
- የተላከው የሪኪምፎርሽን አርዳታ (RA) ፕሮግራምን በአግባቡ ማክበር ነው።
- በሕዝብ መዝገብ ውስጥ የተካተተ ሲሆን የመረጃ ነፃነት ህግ ማክበር በግልጽ ይላካል። አለበለዚያ የማህበራዊ ዋስትና ቁጥር ይሰረዛል።
- የማህበራዊ ዋስትና ቁጥር በወላጁ ወይም በሕጋዊ አሳዳጊው ሰነድ ወይም መረጃ ውስጥ በሚታይ ግለሰብ ወይም በግልጽ ይላካል።
- ቁጥሩ በግልጽ መስኮቱ በኩል መገለጽ የለበትም ወይም ከግልጽ ውጭ መታየት የለበትም።

ሙሉ የማህበራዊ ዋስትና ቁጥር (SSNs) ኢሜይል እንዳይላክ መደረግ አለበት። በምትኩ፣ የግለሰቡ የመጀመሪያ እና የአያት ስም እና የማህበራዊ ዋስትና ቁጥር አራት አሃዞች አስፈላጊ ከሆነ ኢሜይል መላክ አለባቸው። ሆኖም ግን፣ ከክልል ጎራ ውጭ ላለ አካል፣ state.sd.us፣ ሙሉ የማህበራዊ ዋስትና ቁጥር (SSN) መስጠት አስፈላጊ በሚሆንበት ጊዜ፣ ኢሜይል ምስጢራ ጥቅም ላይ ይውላል።

DLR ሰራተኞች በስልክ ማንኛውንም የማህበራዊ ዋስትና ቁጥር (SSN) ይፋ ማድረግ ወይም ማንኛውንም የማህበራዊ ዋስትና ቁጥር (SSN) የሚገልጽ የድምጽ መልእክት መተው የለባቸውም። የማህበራዊ ዋስትና ቁጥር (SSN) በፋክስ መላክ ካለበት፣ የፋክስ መልእክት የተካተተው መረጃ ልዩ እና ሚስጥራዊ እንዲሆን የታሰበ መሆኑን እና በማስተላለፊያ ወረቀቱ ላይ ለተጠቀሰው ግለሰብ ወይም አካል ብቻ ጥቅም ላይ የሚውል መሆኑን የሚገልጽ “የምስጢር ማስታወቂያ” የያዘ የማስተላለፊያ ወረቀት አብሮ መቅረብ አለበት።

PSSN ዎች የያዙ ሁሉም ሰነዶች ወይም ፋይሎች በአካል ደህንነቱ በተጠበቀ ሁኔታ መቀመጥ አለባቸው። PSSN ቁጥሮች (SSNs) ያልተፈቀደ መዳረሻን ለመከላከል ባልተጠበቁ ኮምፒውተሮች ወይም ሌሎች ኤሌክትሮኒክ መሳሪያዎች ላይ መቀመጥ የለባቸውም። የማህበራዊ ዋስትና ቁጥሮችን ከላፕቶፕ ወይም ከዴስክቶፕ ኮምፒውተር ሲያጠፉ፣ ሰራተኞች ቁጥሩ ሙሉ በሙሉ መሰረዙን ማረጋገጥ አለባቸው፣ ይህም ከሪሳይክል ቢን ውስጥም ጭምር።

PSSN ዎች አጠቃቀም

የማህበራዊ ዋስትና ቁጥር (SSN) ጥቅም ላይ የሚውለው ለሚከተሉት ምክንያቶች ብቻ ነው፡-

1. የፕሮግራሙ ብቁነት ወይም እንደዚህ ባሉ ደመወዝ እና የአበል ክፍያዎች ጉዳዮች ላይ መወሰን፣ ምንም እንኳን በመግቢያው ላይ የክፍያውን አይነት መወሰን ባይቻልም፣ አመልካቹ የሚያገኘው ከሆነ፣ የክፍያውን አይነት መወሰን ባይቻልም፤ እና

የሥራ ስምሪት ድጋፍ ጥቅማ ጥቅሞችን፣ ለችግረኛ ቤተሰቦች ጊዜያዊ ድጋፍ (TANF)፣ ተጨማሪ የአመጋገብ እርዳታ ፕሮግራም (SNAP) እና የሥራ ዕድል የግብር ክሬዲት (WOTC) የሚፈልጉ ግለሰቦች ብቁነት ለመሆን የማህበራዊ ዋስትና ክፍላቸው (SSN) ማቅረብ አለባቸው። የማህበራዊ ዋስትና ህግ ርዕስ XI፣ ክፍል 1137(a)(1) እንዲህ ይላል፡

"ግዛቱ [በዚህ አንቀጽ የመጀመሪያ ዓረፍተ ነገር ላይ የተዘረዘሩትን ፕሮግራሞች] ብቁነት ለማድረግ እንደ ቅድመ ሁኔታ አመልካቹ ለግዛቱ የማህበራዊ ዋስትና መለያ ቁጥር እንዲያቀርብ ይጠይቃል፣ እና ግዛቱ በተጠቀሱት ፕሮግራሞች አስተዳደር ውስጥ እንዲህ ዓይነቱን ቁጥር ይጠቀማል።"

የሚከፈልበት የስራ ልምድ የሚሳተፉ ግለሰቦች መምሪያው በትክክል ሪፖርት ማድረግ እንዲችል የማህበራዊ ዋስትና ቁጥር (SSN) ማቅረብ አለባቸው ደመወዝ እና የW-2 እትም።

2. የፕሮግራም አፈጻጸም መለኪያ ውጤቶችን ለማስላት RA የደመወዝ መዝገቦችን መከታተል።

ፕራውዶ ኤስኤስኤ ንዎች

በ20 CFR §666.150 መሠረት በ SDWORKS መግቢያ ወይም የመስመር ላይ ምዝገባ ወቅት የማህበራዊ ዋስትና ቁጥር (SSN) መጠየቅ አለበት። ሆኖም ግን፣ ደንበኛ የማህበራዊ ዋስትና ቁጥር (SSN) እንዲያቀርብ አይጠበቅበትም። አንድ ደንበኛ የSSN ን ማጋራት ካልፈለገ፣ የውሸት-SSN ሊፈጠር ይችላል። የደንበኛን የማህበራዊ ዋስትና ቁጥር (SSN) ሲጠይቁ፣ የ SDWORKS ስርዓት አጠቃቀም እና ግላዊነት እና ደህንነት መገለጽ አለበት።

በ1974 የግላዊነት ህግ ክፍል 7 (5 USC ክፍል 552a ማስታወሻ (የማህበራዊ ዋስትና ቁጥር ይፋ ማድረግ) መሰረት፣ ይፋ ማድረግ በፌዴራል ህግ የሚጠየቅ ካልሆነ በስተቀር፣ ግለሰቡ የማህበራዊ ዋስትና ቁጥራቸውን (SSN) ለመግለጽ ፈቃደኛ ባለመሆኑ ምክንያት አመልካቾች ህግ የተደነገገውን ማንኛውንም መብት፣ ጥቅም ወይም መብት ውድቅ ተደርጓል አይችሉም። ከላይ በ#1 ላይ ከተገለጹት እቃዎች በስተቀር ፣ የማህበራዊ ዋስትና ቁጥር (SSN) ይፋ ባለማድረግ አገልግሎት ውድቅ ተደርጓል ።

[ወደ ይዘቱ ማውጫ ተመለስ](#)

የመረጃ ልቀት

[ቅጽ 1](#) DLR የጽሑፍ ፈቃድ ሳይኖራቸው ስለግለሰቡ ሁኔታ ወይም ስለ PII መረጃ መስጠት የለባቸውም ።

የህግ አስከባሪ የሚቀርቡ የመረጃ ጥያቄዎች ወይም በሰነድ መጥሪያ የሚቀርቡ ጥያቄዎች ለዲቪዥን ዳይሬክተር እና ለዲኤልአር የሕግ ቡድን መቅረብ አለባቸው። የተጋራ መረጃ ሚስጥራዊነትን መጠበቅ አለበት።

የፌዴራል ኤጀንሲዎች በቦታው ላይ ፍተሻዎችን ወይም አዲሶችን ሲያደርጉ፣ DLR መረጃውን ማቅረብ አለበት፤ እርዳታ ለማግኘት የክፍል ዳይሬክተሩን ያነጋግሩ። ሚስጥራዊ መረጃዎችን ማግኘት የሚችሉ ግለሰቦች በመጀመሪያ ሚስጥራዊነትን የሚገልጽ ስምምነት መፈረም አለባቸው።

20 CFR § 666.150
TEGLs 5-08፣ 39-11፣ 10-24
የ1974ቱ የግላዊነት ህግ ክፍል 7 (5 የዩኤስሲ ክፍል 552a ማስታወሻ (የማህበራዊ ዋስትና ቁጥር ይፋ ማድረግ))
የማህበራዊ ዋስትና ህግ ርዕስ XI፣ ክፍል 1137(U)(1)
የፌዴራል የመረጃ ማቀነባበሪያ ደረጃዎች 140-2 ሐ
የ2004 የማህበራዊ ዋስትና ጥበቃ ህግ ወይም የ1974 የግላዊነት ህግ
የመረጃ ነፃነት ህግ

[ወደ ይዘቱ ማውጫ ተመለስ](#)

ይህ ትርጉም የተፈጠረው በማሻን መማሪያ/አርቲፊሻል ኢንተላጂንስ በመጠቀም ሲሆን ለትክክለኛነቱም ተገምግሟል። ሆኖም ግን፣ ስህተቶች ወይም ስህተቶች ካገኙ፣ እባክዎን የትርጉሙን ትክክለኛነት ወይንም ማሻሻል እንድንችል ያሳውቁን።