

CS-13-194

RECEIVED

(Contract Management Use only)

CONTRACT APPROVAL FORM

CONTRACT TRACKING NO.
Cm2121

CONTRACTOR INFORMATION

2014 MAY 21 AM 10:01

Name: X-Celerated DNA & Drug Screenings
 Address: 36 S. Semoran Blvd., Suite B, Orlando, Florida 32807
 Contractor's Administrator Name: Pedro Lebron Title: General Manager
 Tel#: 407-212-3003 Fax: 407-347-4102 Email: plebron@xddsinc.com

CONTRACT INFORMATION

Contract Name: Employee Background Screenings Contract Value: Varies, Estimated \$3,000 annually
 Brief Description: Services for completing new hire background screenings as well as annual MVRs
 Contract Dates : From: May 13, 2014 ^{June 15, 2014} Status: New Renew Amend# WA/Task Order
 How Procured: Sole Source Single Source ITB RFP RFQ Coop. Other

If Processing an Amendment:

Contract #: _____ Increase Amount of Existing Contract: _____ No Increase
 New Contract Dates: _____ to _____ TOTAL OR AMENDMENT AMOUNT: _____

APPROVALS PURSUANT TO NASSAU COUNTY PURCHASING POLICY, SECTION 6

- Chili A Pope 5/21/14
Department Head Signature Date
- Charlotte Young 6/12/14
Contract Management Date
- [Signature] 6-17-14
Office of Management & Budget Date
- [Signature] 6/27/14
County Attorney (approved as to form only) Date

Varies By Department Usage
 Funding Source/Acct #
549081 Background check

Comments: _____

COUNTY MANAGER - FINAL SIGNATURE APPROVAL

Ted Selby [Signature] 7/1/14
 Date

RETURN ORIGINAL(S) TO CONTRACT MANAGEMENT FOR DISTRIBUTION AS FOLLOWS:

- Original: Clerk's Services; Contractor (original or certified copy)
 Copy: Department
 Office of Management & Budget
 Contract Management
 Clerk Finance

14 JUN 18 AM 11:13

14 JUN 30 AM 9:01

14 JUN 12 PM 2:48

CONTRACT MANAGEMENT

RECEIVED COUNTY MANAGERS OFFICE

RECEIVED

RECEIVED COUNTY MANAGERS OFFICE 14 JUL -2 AM 11:02

RECEIVED COUNTY MANAGERS OFFICE 14 MAY 21 AM 8:41

RECEIVED COUNTY MANAGERS OFFICE



Service Agreement

THIS AGREEMENT is made this 15th Day of June 2014 by and between **Nassau County**, and X-celerated DNA & Drug Screenings, Inc. (XDDS).

Client agrees to pay the following services beginning on June 15th, 2014.
 Client may terminate this agreement at any time upon 30 days with a written notice.

- **Criminal County Background\$8.00**
- **Criminal State Background\$9.50**
- **Criminal Federal Background\$10.50**
- **Workman's Compensation\$10.50**
- **Motor Vehicle Report (3) Year.....\$10.75**
(State of Florida)
- **Motor Vehicle Report (7) Year.....\$14.00**
(State of Florida)
- **Educational Background\$9.50**

Please Note: All prices listed above are guaranteed for 1 year. A (60) sixty day notification will be provided prior to any price increase for any and all services. There are no additional or hidden fees applicable. Annual Contract Renewal Required on or before the execution date listed below.

All reports are provided by:

XDDS – S. SEMORAN
 36th S. Semoran Blvd. Suite B,
 Orlando, FL 32807
 Phone: (407) 212-3004
 Fax: (407) 347-4102

XDDS – COLLEGE PARK
 5021 Eggleston Ave. Suite A,
 Orlando, FL 3804
 Phone: (407) 212-3003
 Fax: (407) 347-4102

Please Note: All reports are instantly available. XDDS, Inc. requires a (2) two hour turnaround time in order to verify data reporting out.

XDDS agrees to provide the following:

- Criminal County Background
- Criminal State Background
- Criminal Federal Background
- Workman's Compensation Check
- Motor Vehicle Report (MVR)
- Educational Background



By signing this agreement, I represent that I am an authorized officer of **Nassau County**, with the power to execute this agreement and agree to the terms and conditions stated here.

Nassau County

Print Name: Ted Selby

Signature: [Handwritten Signature]

Title: County Manager

Date: 7/1/14

X-Celerated DNA & Drug Screenings, Inc.

Print Name: Pedro Lebron

Signature: [Handwritten Signature]

Title: President

Date: 6/7/2014

Comparison of Background Quotes

April 2014

Florida	First Advantage	Xcelerated DNA	SingleSource	MAF
County Criminal	\$ 14.50	\$ 8.00	\$ 7.95	\$ 8.00
Surcharge	\$ -	\$ -	\$ -	\$ 14.00
Total	\$ 14.50	\$ 8.00	\$ 7.95	\$ 22.00
Federal Criminal	\$ 14.50	\$ 10.50	\$ 9.00	\$ 8.00
Surcharge	\$ -	\$ -	\$ -	\$ -
Total	\$ 14.50	\$ 10.50	\$ 9.00	\$ 8.00
State Criminal	\$ 14.50	\$ 9.50	\$ 9.00	\$ 5.00
Surcharge	\$ 24.00	\$ -	\$ 33.00	\$ 24.00
Total	\$ 38.50	\$ 9.50	\$ 42.00	\$ 29.00
MVR	\$ 6.50	\$ 14.00	\$ 3.00	\$ 3.00
Surcharge	\$ 10.02	\$ -	\$ 11.10	\$ 10.10
Total	\$ 16.52	\$ 14.00	\$ 14.10	\$ 13.10
Workers Comp	\$ 15.00	\$ 9.50	\$ 9.00	\$ 10.00
Surcharge	\$ -	\$ -	\$ 9.00	\$ -
Total	\$ 15.00	\$ 9.50	\$ 18.00	\$ 10.00
TOTAL FOR FLORIDA	\$ 99.02	\$ 51.50	\$ 91.05	\$ 82.10

Georgia	First Advantage	Xcelerated DNA	SingleSource	MAF
County Criminal	\$ 14.50	\$ 8.00	\$ 7.95	\$ 8.00
Surcharge	\$ -	\$ -	\$ -	\$ -
Total	\$ 14.50	\$ 8.00	\$ 7.95	\$ 8.00
Federal Criminal	\$ 14.50	\$ 10.50	\$ 9.00	\$ 8.00
Surcharge	\$ -	\$ -	\$ -	\$ -
Total	\$ 14.50	\$ 10.50	\$ 9.00	\$ 8.00
State Criminal	\$ 14.50	\$ 9.50	\$ 9.00	\$ 5.00
Surcharge	\$ 2.00	\$ -	\$ 15.00	\$ 15.00
Total	\$ 16.50	\$ 9.50	\$ 24.00	\$ 20.00
MVR	\$ 6.50	\$ 14.00	\$ 3.00	\$ 3.00
Surcharge	\$ 8.00	\$ -	\$ 9.00	\$ 8.00
Total	\$ 14.50	\$ 14.00	\$ 12.00	\$ 11.00
Workers Comp	N/A	N/A	N/A	N/A
Surcharge	N/A	N/A	N/A	N/A
Total	\$ -	\$ -	\$ -	\$ -
TOTAL FOR GEORGIA	\$ 60.00	\$ 42.00	\$ 52.95	\$ 47.00

Education	\$ 21.00	\$ 9.50	\$ 8.00	\$ 9.00
Surcharge	VARIES	\$ -	VARIES	VARIES
Total	\$ 21.00	\$ 9.50	\$ 8.00	\$ 9.00

**Procurement For Background Screening
List of Vendors Request to Quote Was Sent To**

Single Source

FAX: 1-877-835-5787

Phone: 1-800-713-3412

Merchants Association of Florida (MAF)

Nelson San Pedro

Email: nsanpedro@sarma.com

Phone: 813-8923963

American DataBank

FAX: 303-573-1298

Phone: 800-200-0853

X-celerated DNA & Drug Screening (Bid List)

Pedro Lebron

Email: info@xceleratedscreening.com

Phone: 866-483-3337

Request for Quotation Form: Written
Nassau County Board of County Commissioners

Requesting Department: Human Resources

Date: 03/24/2014

Department Address: 96135 Nassau Place, Suite 5
Yulee, Florida 32097

Contact: Tina Keiter (Human Resources Coordinator)

Contact email: tkeiter@nassaucountyfl.com

Department Phone: (904) 491-7332

Department Fax: (904) 321-5797

Product(s)/Service(s) to be purchased (list all specifications and requirements):

Nassau County is seeking quotes from qualified background service providers to provide services to Nassau County BOCC for the attached services.

Please submit written response by: April 11, 2014
(Date)

To be completed by vendor:

Vendor Name: _____

Address: _____

Phone: _____

Fax: _____

Contact: _____

Email: _____

Attached is a written quote from our company, which is valid for _____ days.

Signature

Date

Comments: _____

Request for Written Quotes

Background Services Requested

1. **Criminal County Background**
2. **Criminal State Background**
3. **Criminal Federal Background**
4. **Worker's Compensation**

* The above is required for all new hires, on average, 4 a month, based on 6 months of invoice history.

5. **Motor Vehicle Check Background**

* This is performed on all new hires as well as other circumstances. On average, 5 a month, based on 6 months of invoice history.

6. **Educational Background**

*These are only required for new hires who fill a position requiring a degree, these are rare, less than 1 a month, based on 6 months of invoice history.

Please quote on the following:

1. **We are aware that costs will vary from State to State, thus please quote total prices for all of the above for both Florida and Georgia as those are the most common in our area. (Please break out to include your fee as well as any pass through fees.)**
2. **Any start up fees, if applicable.**
3. **The timeframe to receive reports once an order has been placed.**

**Procurement For Background Screening
List of Vendors Request to Quote Was Sent To**

Single Source

FAX: 1-877-835-5787

Phone: 1-800-713-3412

Merchants Association of Florida (MAF)

Nelson San Pedro

Email: nsanpedro@sarma.com

Phone: 813-8923963

American DataBank

FAX: 303-573-1298

Phone: 800-200-0853

X-celerated DNA & Drug Screening (Bid List)

Pedro Lebron

Email: info@xceleratedscreening.com

Phone: 866-483-3337

Request for Quotation Form: Written
Nassau County Board of County Commissioners

Requesting Department: Human Resources

Date: 03/24/2014

Department Address: 96135 Nassau Place, Suite 5
Yulee, Florida 32097

Contact: Tina Keiter (Human Resources Coordinator)

Contact email: tkeiter@nassaucountyfl.com

Department Phone: (904) 491-7332

Department Fax: (904) 321-5797

Product(s)/Service(s) to be purchased (list all specifications and requirements):

Nassau County is seeking quotes from qualified background service providers to provide services to Nassau County BOCC for the attached services.

Please submit written response by: April 11, 2014
(Date)

To be completed by vendor:

Vendor Name: _____
Address: _____
Phone: _____
Fax: _____
Contact: _____
Email: _____

Attached is a written quote from our company, which is valid for _____ days.

Signature Date

Comments: _____

Request for Written Quotes

Background Services Requested

1. **Criminal County Background**
2. **Criminal State Background**
3. **Criminal Federal Background**
4. **Worker's Compensation**

* The above is required for all new hires, on average, 4 a month, based on 6 months of invoice history.

5. **Motor Vehicle Check Background**

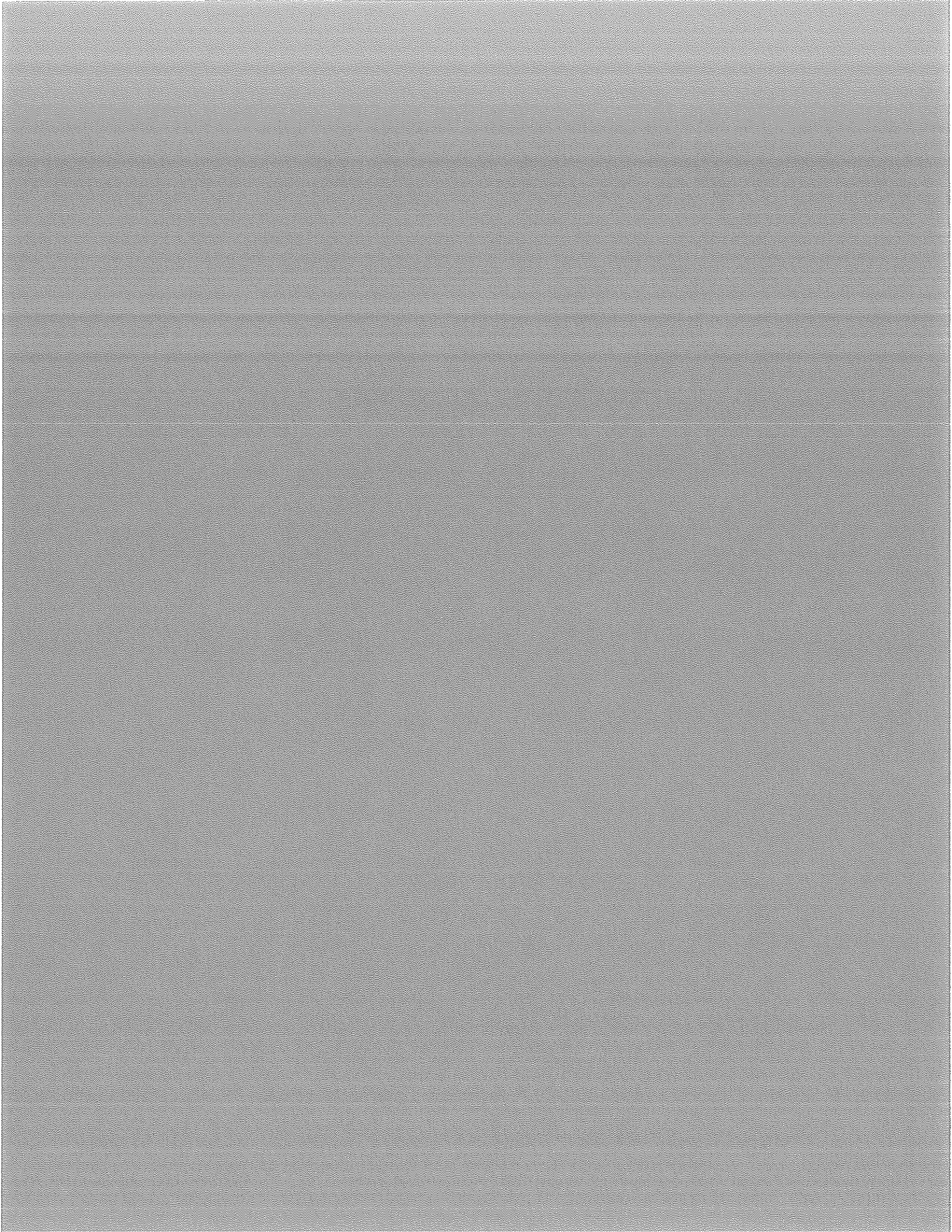
* This is performed on all new hires as well as other circumstances. On average, 5 a month, based on 6 months of invoice history.

6. **Educational Background**

*These are only required for new hires who fill a position requiring a degree, these are rare, less than 1 a month, based on 6 months of invoice history.

Please quote on the following:

1. **We are aware that costs will vary from State to State, thus please quote total prices for all of the above for both Florida and Georgia as those are the most common in our area. (Please break out to include your fee as well as any pass through fees.)**
2. **Any start up fees, if applicable.**
3. **The timeframe to receive reports once an order has been placed.**



Request for Quotation Form: Written
Nassau County Board of County Commissioners

Requesting Department: Human Resources

Date: 03/24/2014

Department Address: 96135 Nassau Place, Suite 5
Yulee, Florida 32097

Contact: Tina Keiter (Human Resources Coordinator)
Contact email: tkeiter@nassaucountyfl.com
Department Phone: (904) 491-7332
Department Fax: (904) 321-5797

Product(s)/Service(s) to be purchased (list all specifications and requirements):

Nassau County is seeking quotes from qualified background service providers to provide services to Nassau County BOCC for the attached services.

Please submit written response by: April 11, 2014
(Date)

To be completed by vendor:

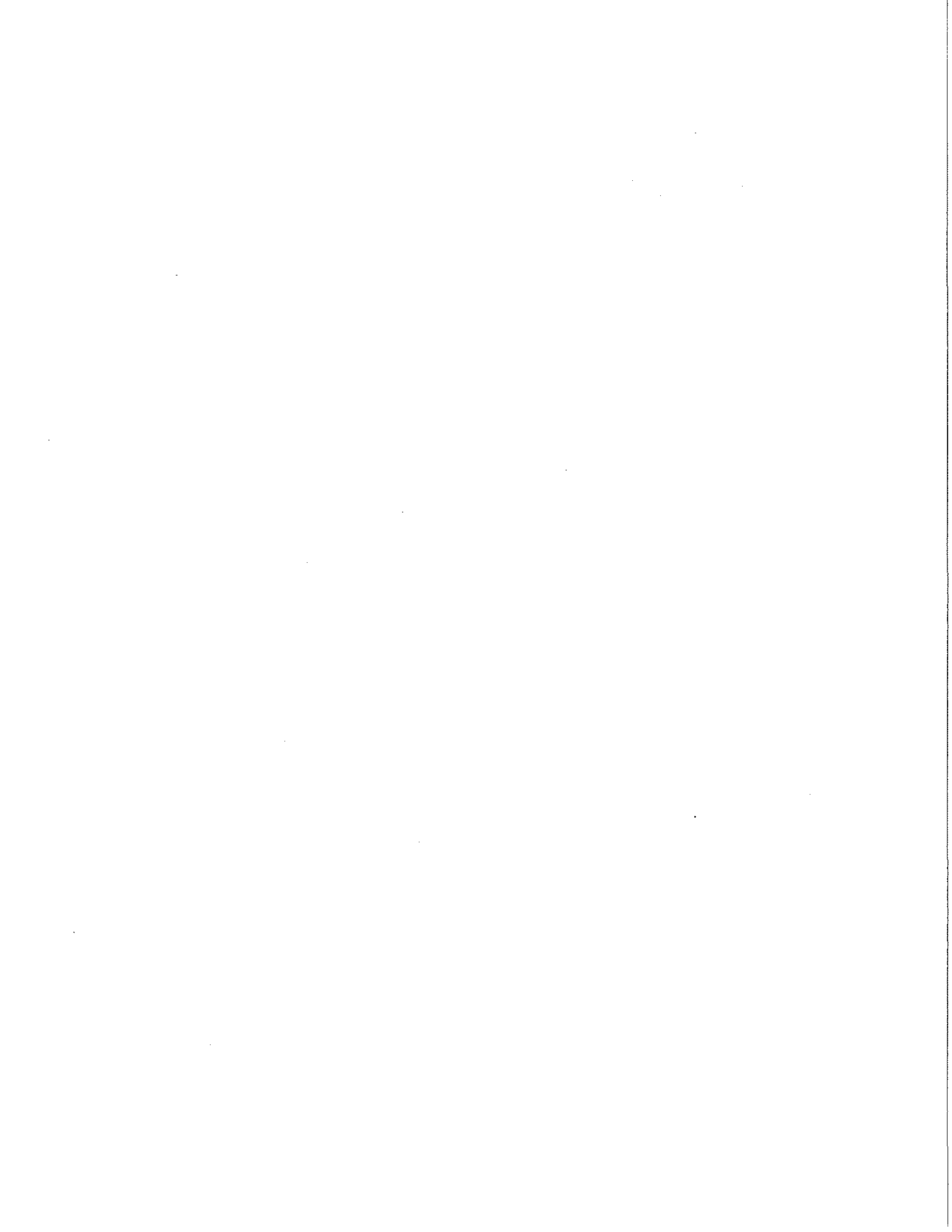
Vendor Name: Xcelerated DNA + Drug Screenings, Inc.
Address: 36 S. Semoran Blvd
Suite B, Orlando, FL 32807
Phone: (407) 212-3603
Fax: 407 247-4102
Contact: Pedro Lebron
Email: plebron@xddsinc.com

Attached is a written quote from our company, which is valid for 60 days.

Pedro Lebron
Signature

3/25/2014
Date

Comments: _____



Tina Keiter

From: Pedro Lebron <plebron@xddsinc.com>
Sent: Thursday, April 17, 2014 11:13 AM
To: Tina Keiter
Subject: RE: Quote for Services

Yes please...the 7 year reports we can do for \$14.00

[CLICK ME!](#)



Pedro Lebron
General Manager

X-New XDDS Location!
S. Semoran Location
36 S. Semoran Boulevard, STE. B
Orlando, FL 32807
407-212-3004 Off.
407-347-4102 Fax.

From: Tina Keiter [mailto:tkeiter@nassaucountyfl.com]
Sent: Thursday, April 17, 2014 10:26 AM
To: Pedro Lebron
Subject: RE: Quote for Services

Mr. Lebron –

I'm sorry to bother you again, but I'm going through these quotes and noticed when we were talking before that you mentioned the state fee for an MVR is \$8.12 so I have noticed in another bid that is for a 3 year and we do 7 years which looks to be \$10.....just want to see if given the fact that we do 7 years and since I didn't mention that in the request for quotes if you want me to adjust the cost of the MVR for your company.

Thanks so much for your help!

Tina L. Keiter

Nassau County Human Resources
96135 Nassau Place, Suite 5
Yulee, Florida 32097
Phone: 904-491-7332
FAX: 904-321-5797

Confidentiality Notice

Tina Keiter

From: Pedro Lebron [plebron@xddsinc.com]
Sent: Tuesday, March 25, 2014 12:55 PM
To: Tina Keiter
Subject: RE: Quote for Services

Sorry.....I am in the field and you know how this smart phones are.....

Sent from my T-Mobile 4G LTE Device

----- Original message -----

From: Tina Keiter
Date: 03/25/2014 12:46 PM (GMT-05:00)
To: Pedro Lebron
Subject: RE: Quote for Services

Haha.....Thank you!

Tina L. Keiter

Nassau County Human Resources

Confidentiality Notice

This communication is intended only for the use of the addressee and may contain information that is privileged and confidential.

If you are not the intended recipient, you are hereby notified that the unauthorized dissemination of this communication is

strictly prohibited. If you have received this communication in error; please notify us immediately by phone. Thank you.

From: Pedro Lebron [mailto:plebron@xddsinc.com]
Sent: Tuesday, March 25, 2014 12:44 PM
To: Tina Keiter
Subject: RE: Quote for Services

3/25/2014

Np prblem....yes...the same way

Sent from my T-Mobile 4G LTE Device

----- Original message -----

From: Tina Keiter

Date:03/25/2014 12:21 PM (GMT-05:00)

To: Pedro Lebron

Subject: RE: Quote for Services

Thank you so very much, that's the same w/ all the background checks, correct? Not just MVRs? Forgive me; I just want to make sure I'm comparing apples to apples.....

Tina L. Keiter

Nassau County Human Resources

Confidentiality Notice

This communication is intended only for the use of the addressee and may contain information that is privileged and confidential.

If you are not the intended recipient, you are hereby notified that the unauthorized dissemination of this communication is

strictly prohibited. If you have received this communication in error; please notify us immediately by phone. Thank you.

From: Pedro Lebron [mailto:plebron@xddsinc.com]
Sent: Tuesday, March 25, 2014 12:13 PM

3/25/2014

To: Tina Keiter
Subject: RE: Quote for Services

Mrs. Kelter,

My fees actually include the state fees.....

FYI....the MVR Fee in the state of Florida is \$8.12. Some companies like to increase the state fees in order to increase profit.

Just to confirm. Each and every time you order an MVR Report the total and only amount to be billed will be \$10.75. Please let me know if you have any other questions.

Also, our reports are thru American Driving Records. I can provide a sample report if you like one at no cost.

We at XDDS look forward to working with Nassau County.

Thanks again!

[CLICK ME!](#)



Pedro Lebron
General Manager

3/25/2014

X-New XDDS Location!

S. Semoran Location

36 S. Semoran Boulevard, STE. B

Orlando, FL

407-212-3004 Off.

407-347-4102 Fax.

From: Tina Keiter [mailto:tkeiter@nassaucountyfl.com]
Sent: Tuesday, March 25, 2014 12:02 PM
To: Pedro Lebron; XDDS Info
Subject: RE: Quote for Services

Mr. Lebron –

Thank you so very much for your prompt response. Could I please verify just one thing though? Are these prices all inclusive, i.e. we currently pay the company we have a fee to complete an MVR, however the State of Florida charges them \$10.02 for them to run it, thus we pay total of the two combined costs. Can we expect to have additional costs to this quote as well or does this include any fess the State might charge and this is the total cost we'll pay?

Thanks, so much,

Tina L. Keiter

Nassau County Human Resources

Confidentiality Notice

3/25/2014

This communication is intended only for the use of the addressee and may contain information that is privileged and confidential.

If you are not the intended recipient, you are hereby notified that the unauthorized dissemination of this communication is

strictly prohibited. If you have received this communication in error; please notify us immediately by phone. Thank you.

From: Pedro Lebron [<mailto:plebron@xddsinc.com>]
Sent: Tuesday, March 25, 2014 11:47 AM
To: Tina Keiter; XDDS Info
Subject: RE: Quote for Services

Hello Tina,

Thank you for the bid invitation below. Please see attached Quote along with completed vendor information. Please let me know if you have any questions or concerns.

Sincerely,

[CLICK ME!](#)



Pedro Lebron
General Manager

3/25/2014

X-New XDDS Location!

S. Semoran Location

36 S. Semoran Boulevard, STE. B

Orlando, FL

407-212-3004 Off.

407-347-4102 Fax.

From: Tina Keiter [<mailto:tkeiter@nassaucountyfl.com>]

Sent: Monday, March 24, 2014 4:39 PM

To: XDDS Info

Subject: Quote for Services

Mr. San Pedro –

Please see attached a request for quote for Nassau County's background services.

If you need any additional information, please let me know.

Thanks,

Tina L. Keiter

Nassau County Human Resources

96135 Nassau Place, Suite 5

Yulee, Florida 32097

Phone: 904-491-7332

FAX: 904-321-5797

3/25/2014

Confidentiality Notice

This communication is intended only for the use of the addressee and may contain information that is privileged and confidential.

If you are not the intended recipient, you are hereby notified that the unauthorized dissemination of this communication is

strictly prohibited. If you have received this communication in error; please notify us immediately by phone. Thank you.



PROPOSAL

NASSAU COUNTY BACKGROUND CHECK SERVICES

- Criminal County Background.....\$8.00
- Criminal State Background..... \$9.50
- Criminal Federal Background..... \$10.50
- Worker's Compensation..... \$10.50
- Motor Vehicle Check..... \$10.75
- Educational Background..... \$9.50

*** All reports are instantly available. X-celerated DNA & Drug Screenings, Inc. (XDDS) prefers a (2) two hour turnaround time in order to verify accuracy of data being reported. There is no start up fees. Fees are only applicable when reports are ordered. Billing can be completely customizable to fit your needs. Orders can be placed via email, fax, or on our website at www.XDDSInc.com Details and procedures will be provided following our agreement along with a customized Background Authorization Form ***

36 S. Semoran Blvd. Suite B/ Orlando, FL 32807
(407) 212-3003 Main / (407) 347-4102 Fax
info@xddsinc.com / www.XDDSInc.com

Tina Keiter

From: Pedro Lebron [plebron@xddsinc.com]

Sent: Tuesday, March 25, 2014 12:03 PM

To: Tina Keiter

Subject: Out of Office: Quote for Services

Attention!

X-celerated DNA & Drug Screenings is permanentaly moving to its Semoran location located at:

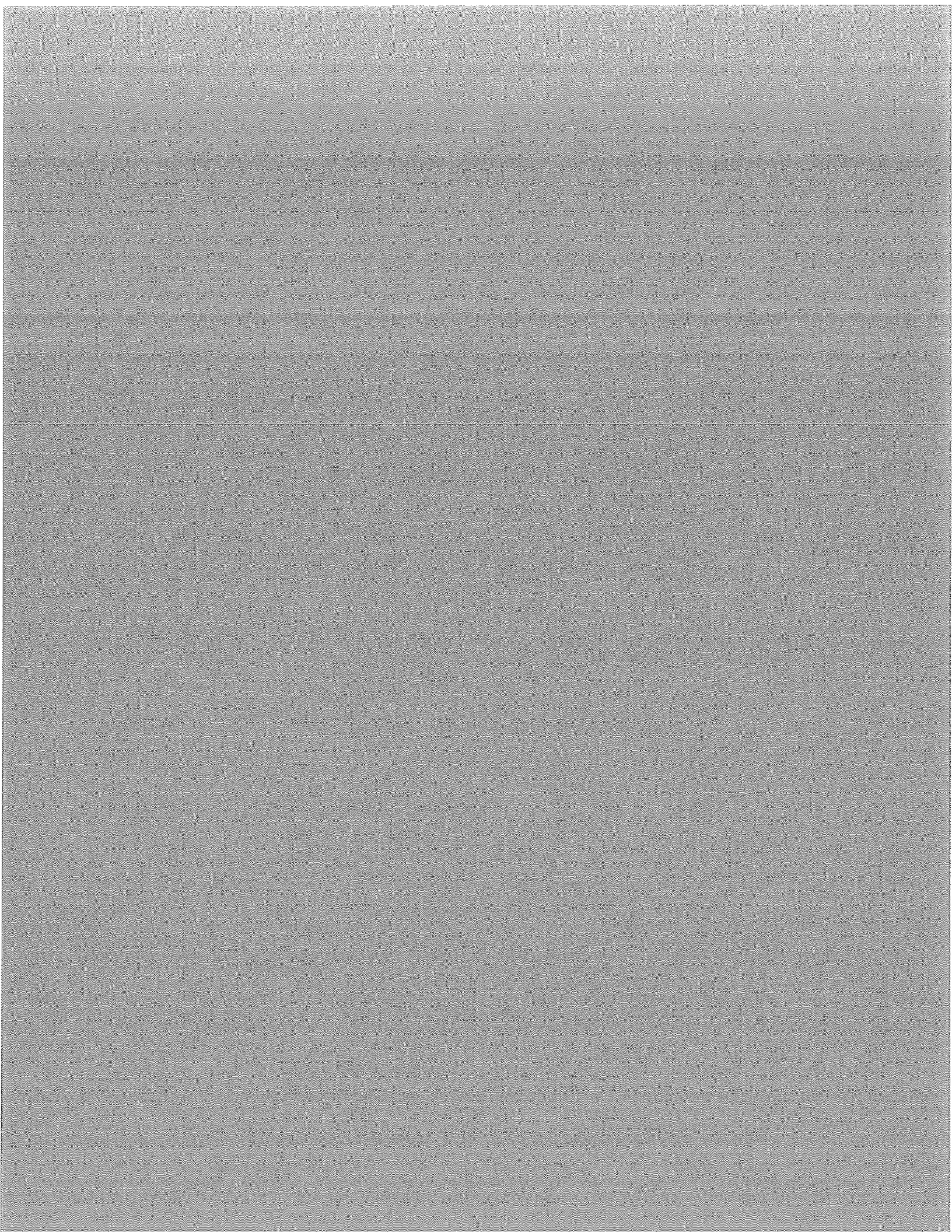
**36 S. Semoran Blvd. Suite B
Orlando, FL 32804**

Please change your records accordingly.

Thank you,

Pedro Lebron
General Manager

3/25/2014





Nassau County BOCC: Proposal

Company Overview

SingleSource Services began as a background screening and security firm, serving organizations of every type and size. We offer a secure and comprehensive suite of people management tools, Internet-based software that is supported by a team of professionals. SingleSource contributes to the success of its constituents with integrity, confidentiality and professionalism in providing comprehensive, FCRA compliant background checks with the ability to adapt to ever changing requirements and client needs.

SingleSource is a founding member of National Association of Professional Background Screeners (NAPBS) and a member of Concerned CRAs, a group of ethical background screening vendors who maintain the highest standards of truth in business and have made it their goal to ensure that employers are aware of the strengths and weaknesses of database searches.

- Official registered name (Corporate, D.B.A., Partnership, etc.), address, main telephone number, toll-free numbers, and facsimile numbers.

SingleSource Services Corporation,
2320 South Third Street, Suite 7
Jacksonville Beach, Florida 32250.
Telephone: (800) 713-3412 ext. 135
Fax: (877) 835-5787

- Key contact name, title

Mandi Stephens, Client Support.

Product Information and Pricing - Programs

- **Discovery Plus with Criminal Package** (3 counties included in price) \$31.00*
This package is the staple in respect to employment screening and represents the best value and is the most effective. ** Searches are conducted in all counties of residence for prior 7 years. Multi-jurisdictional Database Search, Residence Trace & Federal Criminal Search are included in your package.
- **Discovery Plus with Criminal and Educational Background Package** (3 counties included in price) \$39.00*
This package is the staple in respect to employment screening and represents the best value and is the most effective. ** Searches are conducted in all counties of residence for prior 7 years. Multi-jurisdictional Database Search, Residence Trace & Federal Criminal Search, and one education verification are included in your package.

Product Information and Pricing – Individual inquiries

County Criminal Search \$7.95 each (see attached access fee table for FL and GA)

May return records of any cases where the subject name matches that of a court record. Identifiers such as date of birth (DOB), social security number (SSN), address etc. are usually obtained. Misdemeanors are not always included.

Federal Criminal Search \$9.00 each

May return records of cases filed in Federal Court Jurisdictions. These would be Federal crimes as opposed to state crimes.

Driving History State DMV Records \$3.00* each (FL \$11.10 & GA \$9.00 including access)

The driving history for the subject is obtained from the state of current licensure. Since most states only allow a short period of time to obtain a driving license upon moving to the state this is usually the state of current residency. If it is not then questions should be asked, since all states do not have reciprocity and there may be reasons for not wanting a license in the current state of residency. Likewise previous state histories may be advisable (compulsory in the case of DOT drivers). The presence of a poor driving history may indicate a lack of responsibility or regard for rules. May also include DOB, SSN, description of subject etc. Driving License Number is required. Some states require a signed release on a special form, and the records are available in most states. The driving history transcript is provided as an original document. A state fee is payable that varies by state. Default search (usually 3 years) conducted unless otherwise specified.

Statewide Criminal \$9.00* each (FL \$33.00 & GA \$15.00 including Access fees)

May return records of arrests and/or convictions that have been notified to the state repository. Records from some states report records that have not resulted in charges or convictions. Some states require signed releases. Some states reports are police reports and not court reports. Misdemeanors are not always included. Many states do not hold all data available at county courts. Problems with data flow to state records from police departments, sheriff's offices and courts sometimes mean that data is incomplete or missing.

Education Validation \$8.00*** each

This inquiry verifies that the subject received the degree or diploma that he/she claims and that it is issued by a valid institution and not Diploma Mill. There are hundreds of known diploma mills with new ones appearing regularly. Some schools use education verification databases and these are billed at cost.

Worker's Compensation \$9.00* each (No access fees for FL or GA)

Searches the state bureau for worker's compensation records for current and past lost time, as well as medical claims. (Not available in all states)

* Access or Additional Fees May Apply (Complete table of FL & GA Access fees attached).

** If additional county criminal search need be conducted - \$7.95 per additional county.

*** Some schools use educational clearing houses resulting in an additional fee which SSS bills at cost.

SingleSource has zero sign up fees, no monthly, annual or minimum usage fees for background screening services.

2320 S. THIRD ST., STE 7, JACKSONVILLE BEACH, FL 32250

P: 800-713-3412 F: 877-835-5787

www.SingleSourceServices.com

Georgia Access Fees

Search	County	State	Fee	Date Entered	Last Updated
Driving History - 3 Years	Statewide	GA	\$6.00	10/3/2007	7/15/2009
Driving History - 7 Years	Statewide	GA	\$8.00	10/3/2007	7/15/2009
Statewide Criminal	Statewide	GA	\$6.00	6/8/2004	10/26/2007

Florida Access Fees

Search	County	State	Fee	Date Entered	Last Updated
10 Year Felony/Misdemeanor	Bradford	FL	\$20.00	4/6/2011	4/6/2011
10 Year Felony/Misdemeanor	Hardee	FL	\$20.00	12/28/2011	12/28/2011
10 Year Felony/Misdemeanor	Jackson	FL	\$20.00	7/29/2004	7/29/2004
10 Year Felony/Misdemeanor	Suwannee	FL	\$20.00	8/29/2011	8/29/2011
10 Year Felony/Misdemeanor	Taylor	FL	\$20.00	7/29/2004	7/29/2004
7 Year Felony/Misdemeanor	Bradford	FL	\$14.00	4/6/2011	4/6/2011
7 Year Felony/Misdemeanor	Franklin	FL	\$14.00	1/11/2005	1/11/2005
7 Year Felony/Misdemeanor	Hamilton	FL	\$14.00	3/20/2013	3/20/2013
7 Year Felony/Misdemeanor	Hardee	FL	\$14.00	12/28/2011	12/28/2011
7 Year Felony/Misdemeanor	Jackson	FL	\$14.00	7/20/2004	5/30/2008
7 Year Felony/Misdemeanor	Lafayette	FL	\$14.00	1/11/2005	1/11/2005
7 Year Felony/Misdemeanor	Liberty	FL	\$14.00	9/17/2004	9/17/2004
7 Year Felony/Misdemeanor	Suwannee	FL	\$14.00	8/29/2011	8/29/2011
7 Year Felony/Misdemeanor	Taylor	FL	\$14.00	7/29/2004	7/29/2004
Courier Fee	Dade	FL	\$15.00	10/24/2007	10/24/2007
Discovery Verification	Hamilton	FL	\$14.00	3/20/2013	3/20/2013
Discovery Verification	Taylor	FL	\$14.00	10/28/2012	10/28/2012
Driving History - 3 Years	Statewide	FL	\$8.10	10/3/2007	7/15/2009
Driving History - 7 Years	Statewide	FL	\$10.10	10/3/2007	7/15/2009
Statewide Criminal	Statewide	FL	\$24.00	3/18/2005	6/30/2008

Tina Keiter

From: Mandi Stephens <MStephens@singlesourceservices.com>
Sent: Thursday, April 17, 2014 5:09 PM
To: Tina Keiter
Cc: Nikki Faulkner
Subject: RFP - Nassau County Board of County Commissioners / SingleSource Services
Attachments: Revicسد Proposal for Nassau County BOCC.pdf

Good evening Tina,


Attached is the revision of our original proposal. Thank you so very much for this opportunity, and hopefully we will hear from you very soon!

Enjoy the weekend.

Kind Regards,
Mandi Stephens
Client Support
T -800-713-3412 x118
F -877-835-5787
www.SingleSourceServices.com

SingleSource 
Trusted background screening since 1995

2320 South Third Street | Suite 7
Jacksonville Beach | Florida | 32250

napbs
FCRA  Basic
Certification

SINCE 1995 your trusted source for Background Screening & Drug Testing.

We also offer Paperless I9 and E-Verify, Exit Interviews & Surveys, HRVerifications Cash Back Program and now ArrestAlarm

P Please consider the environment before printing this e-mail

This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 U.S.C. Sec. 2510-2521.

NOTHING IN THIS EMAIL SHALL BE CONSTRUED AS LEGAL ADVICE AND THE GUIDANCE OF COUNSEL SHOULD BE SOUGHT BEFORE TAKING ANY ACTION BASED UPON IT.

From: Nikki Faulkner
Sent: Thursday, April 17, 2014 9:37 AM
To: Mandi Stephens
Subject: FW: RFP - Nassau County Board of County Commissioners / SingleSource Services

From: Tina Keiter [<mailto:tkeiter@nassaucountyfl.com>]
Sent: Thursday, April 17, 2014 9:14 AM
To: Nikki Faulkner
Subject: RE: RFP - Nassau County Board of County Commissioners / SingleSource Services

Ms. Faulkner –

I appreciate your response, however in reviewing the costs note that there is an asterisk which states "Access Fees May Apply". As stated in the request for quote, I need the "total prices for all of the above for both Florida and Georgia as those are the most common in our area. (Please break out to include your fee as well as any pass through fees.)"

If you could please provide a TOTAL of all fees for these services it would be greatly appreciated as I am unable to equitably compare vendors without this information.

I look forward to your response and thank you.

Tina L. Keiter

Nassau County Human Resources
96135 Nassau Place, Suite 5
Yulee, Florida 32097
Phone: 904-491-7332
FAX: 904-321-5797

Confidentiality Notice

This communication is intended only for the use of the addressee and may contain information that is privileged and confidential.

If you are not the intended recipient, you are hereby notified that the unauthorized dissemination of this communication is

strictly prohibited. If you have received this communication in error; please notify us immediately by phone. Thank you.

From: Nikki Faulkner [<mailto:NFaulkner@singlesourceservices.com>]

Sent: Friday, April 11, 2014 6:25 PM

To: Tina Keiter

Cc: Mandi Stephens; Don Dyer

Subject: RFP - Nassau County Board of County Commissioners / SingleSource Services

Vendor Name: SingleSource Services Corporation
Vendor Address: 2320 South 3rd St., Suite 7
Jacksonville Beach, FL 32250
Vendor Phone: 800 713-3412
Vendor Fax: 877 835-5787
Contact: Miranda Stephens
Contact email: mstephens@singlesourceservices.com

Attached is a written quote from our company, which is valid for 120 days.

Please feel free to contact Miranda Stephens (Mandi) or me if you have any questions or if we may be of service in any way.


Best regards,
Nikki Faulkner
Client Support
T -800 713 3412 x 113
F -877 835 5787

www.SingleSourceServices.com

SingleSource 

Trusted background screening since 1995

2320 South Third Street | Suite 7
Jacksonville Beach | Florida | 32250

napbs
FCRA  Basic
Certification

SINCE 1995 your trusted source for Background Screening & Drug Testing.

We also offer Paperless I9 and E-Verify, Exit Interviews & Surveys, HRVerifications Cash Back Program and now ArrestAlarm

 **Please consider the environment before printing this e-mail**

This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 U.S.C. Sec. 2510-2521.

NOTHING IN THIS EMAIL SHALL BE CONSTRUED AS LEGAL ADVICE AND THE GUIDANCE OF COUNSEL SHOULD BE SOUGHT BEFORE TAKING ANY ACTION BASED UPON IT.

Tina Keiter

From: Nikki Faulkner <NFaulkner@singlesourceservices.com>
Sent: Friday, April 11, 2014 6:25 PM
To: Tina Keiter
Cc: Mandi Stephens; Don Dyer
Subject: RFP - Nassau County Board of County Commissioners / SingleSource Services
Attachments: Nassau County RFP 041114.pdf

Vendor Name: SingleSource Services Corporation
Vendor Address: 2320 South 3rd St., Suite 7
Jacksonville Beach, FL 32250
Vendor Phone: 800 713-3412
Vendor Fax: 877 835-5787
Contact: Miranda Stephens
Contact email: mstephens@singlesourceservices.com

Attached is a written quote from our company, which is valid for 120 days.

Please feel free to contact Miranda Stephens (Mandi) or me if you have any questions or if we may be of service in any way.

Best regards,
Nikki Faulkner
Client Support
T -800 713 3412 x 113
F -877 835 5787
www.SingleSourceServices.com

SingleSource
Trusted background screening since 1995
2320 South Third Street | Suite 7
Jacksonville Beach | Florida | 32250

napbs
Basic
FCRA Certification

SINCE 1995 your trusted source for Background Screening & Drug Testing.

We also offer Paperless I9 and E-Verify, Exit Interviews & Surveys, HRVerifications Cash Back Program and now ArrestAlarm

 **Please consider the environment before printing this e-mail**

This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 U.S.C. Sec. 2510-2521.

NOTHING IN THIS EMAIL SHALL BE CONSTRUED AS LEGAL ADVICE AND THE GUIDANCE OF COUNSEL SHOULD BE SOUGHT BEFORE TAKING ANY ACTION BASED UPON IT.



Nassau County BOCC: Proposal

Company Overview

SingleSource Services began as a background screening and security firm, serving organizations of every type and size. We offer a secure and comprehensive suite of people management tools, Internet-based software that is supported by a team of professionals. SingleSource contributes to the success of its constituents with integrity, confidentiality and professionalism in providing comprehensive, FCRA compliant background checks with the ability to adapt to ever changing requirements and client needs.

SingleSource is a founding member of National Association of Professional Background Screeners (NAPBS) and a member of Concerned CRAs, a group of ethical background screening vendors who maintain the highest standards of truth in business and have made it their goal to ensure that employers are aware of the strengths and weaknesses of database searches.

- Official registered name (Corporate, D.B.A., Partnership, etc.), address, main telephone number, toll-free numbers, and facsimile numbers.

SingleSource Services Corporation,
2320 South Third Street, Suite 7
Jacksonville Beach, Florida 32250.
Telephone: (800) 713-3412 ext. 135
Fax: (877) 835-5787

- Key contact name, title

Mandi Stephens, Client Support.

Product Information and Pricing - Programs

- **Discovery Plus with Criminal Package** (3 counties included in price) \$31.00*
This package is the staple in respect to employment screening and represents the best value and is the most effective. ** Searches are conducted in the all counties of residence for prior 7 years. Multi-jurisdictional Database Search, Residence Trace & Federal Criminal Search are included in your package.
- **Discovery Plus with Criminal and Educational Background Package** (3 counties included in price) \$39.00*
This package is the staple in respect to employment screening and represents the best value and is the most effective. ** Searches are conducted in the all counties of residence for prior 7 years. Multi-jurisdictional Database Search, Residence Trace & Federal Criminal Search, and one education verification are included in your package.

Product Information and Pricing – Individual inquiries

- **Federal Criminal Search** \$9.00* each

May return records of cases filed in Federal Court Jurisdictions. These would be Federal crimes as opposed to state crimes.

- **Driving History State DMV Records** \$3.00* each

The driving history for the subject is obtained from the state of current licensure. Since most states only allow a short period of time to obtain a driving license upon moving to the state this is usually the state of current residency. If it is not then questions should be asked, since all states do not have reciprocity and there may be reasons for not wanting a license in the current state of residency. Likewise previous state histories may be advisable (compulsory in the case of DOT drivers). The presence of a poor driving history may indicate a lack of responsibility or regard for rules. May also include DOB, SSN, description of subject etc. Driving License Number is required. Some states require a signed release on a special form, and the records are available in most states. The driving history transcript is provided as an original document. A state fee is payable that varies by state.

- **Education Validation** \$8.00* each

This inquiry verifies that the subject received the degree or diploma that he/she claims and that it is issued by a valid institution and not Diploma Mill. There are hundreds of known diploma mills with new ones appearing regularly. Some schools use education verification databases and these are billed at cost.

- **Statewide Criminal** \$9.00* each

May return records of arrests and/or convictions that have been notified to the state repository. Records from some states report records that have not resulted in charges or convictions. Some states require signed releases. Some states reports are police reports and not court reports. Misdemeanors are not always included. Many states do not hold all data available at county courts. Problems with data flow to state records from police departments, sheriff's offices and courts sometimes mean that data is incomplete or missing.

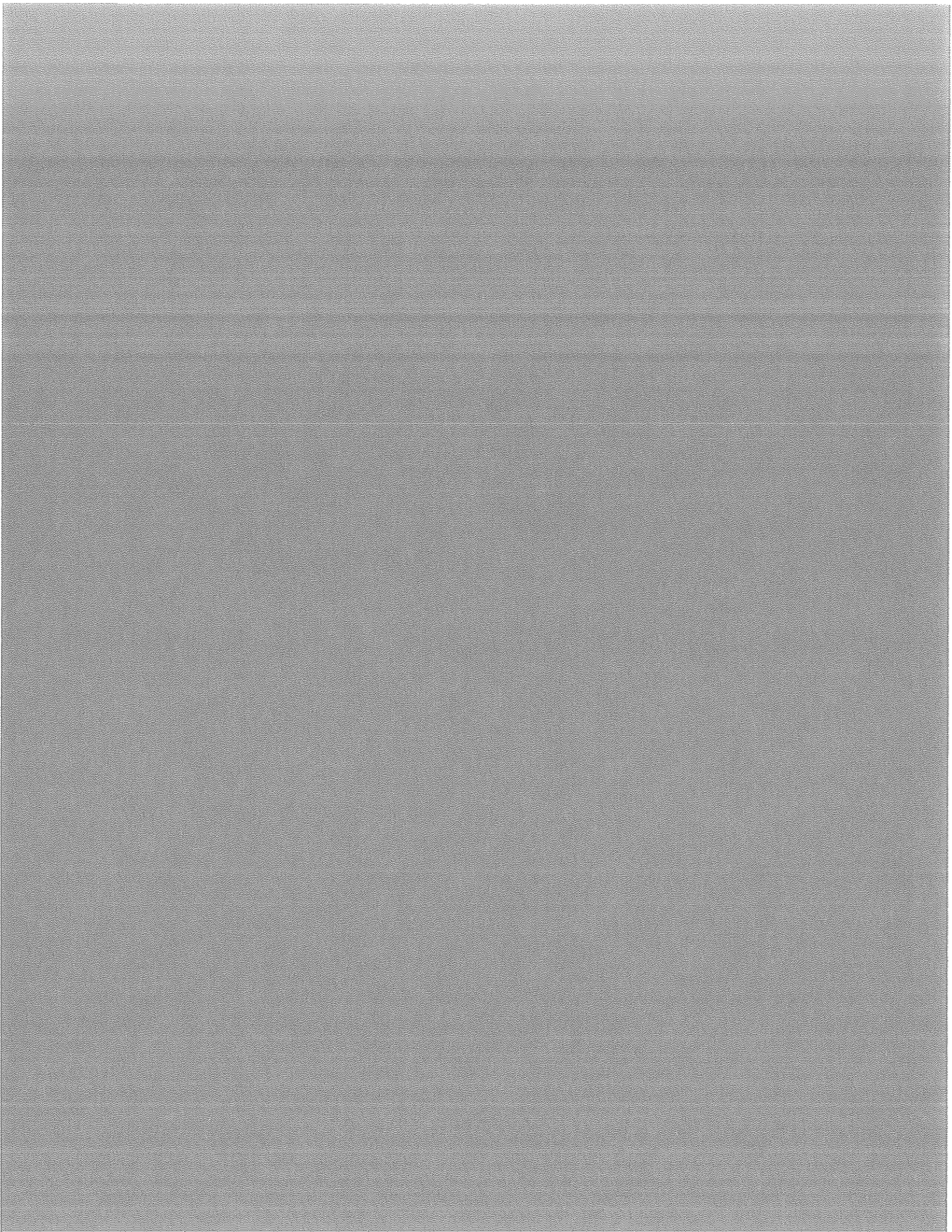
- **Worker's Compensation** \$9.00* each

Searches the state bureau for workman's compensation records for current and post lost time, as well as medical claims.

* Access Fees May Apply

** If additional county criminal search need be conducted - \$7.95 per additional county.

SingleSource has zero sign up fees, no monthly, annual or minimum usage fees for background screening services.



MAF Background ScreeningSM

A Division of Sarma



STATE CRIMINAL FEES

STATE	FEE
-------	-----

Alabama	\$ 10.00
Alaska	n/c
Arizona	n/c
Arkansas	\$ 23.00
California	n/c
Colorado	\$ 14.00
Connecticut	\$ 25.00
Delaware	n/c
District of Columbia	\$ 13.00
Florida	\$ 24.00
Georgia	\$ 15.00
Hawaii	\$ 15.00
Idaho	\$ 23.00
Illinois	\$ 15.00
Indiana	\$ 25.00
Iowa	\$ 23.00
Kansas	\$ 20.00
Kentucky	\$ 20.00
Louisiana	n/c
Maine	n/c
Maryland	\$ 12.00
Massachusetts	\$ 35.00
Michigan	n/c
Minnesota	\$ 12.00
Mississippi	\$ 17.00
Missouri	\$ 9.00

STATE	FEE
-------	-----

Montana	\$ 18.00
Nebraska	\$ 16.00
Nevada	n/c
New Hampshire	\$ 25.00
New Jersey	\$ 15.00
New Mexico	\$ 15.00
New York	\$ 68.00
North Carolina	\$ 12.00
North Dakota	n/c
Ohio	n/c
Oklahoma	\$ 17.50
Oregon	\$ 14.00
Pennsylvania	\$ 10.00
Rhode Island	\$ 15.00
South Carolina	\$ 25.00
South Dakota	\$ 21.00
Tennessee	\$ 35.00
Texas	\$ 10.00
Utah	\$ 14.00
Vermont	n/c
Virginia	\$ 19.00
Washington	\$ 9.00
West Virginia	\$ 20.00
Wisconsin	\$ 13.00
Wyoming	\$ 20.00

*n/c=not covered

Tina Keiter

From: Nelson San Pedro <nelson.sanpedro@mascreeing.com>
Sent: Thursday, April 17, 2014 1:36 PM
To: Tina Keiter
Cc: Nelson San Pedro
Subject: RE: MAF Background Screening-Nassau County-State fees
Attachments: MAF-SARMA STATE REPOSITORY FEES 3-2014.pdf

Importance: High

Hi Tina,

I am sorry, here is the information requested.

Let me know if you need further assistance.

Thanks!

Nelson San Pedro

MAF Background Screening

Phone: (813) 892-3963

Fax: (813) 283-4964

MAF's Operation Center

800-226-4483



Check us out on you tube!

MAF Background Screening a division of Sarma.

From: Tina Keiter [<mailto:tkeiter@nassaucountyfl.com>]
Sent: Thursday, April 17, 2014 12:52 PM
To: Nelson San Pedro
Subject: RE: MAF Background Screening-Nassau County

Nelson –

I've been going through your quote this morning and it looks like I have everything except the surcharges for the State backgrounds, could you please let me know what those charges will be for Florida and Georgia?

Request for Quotation Form: Written
Nassau County Board of County Commissioners

Requesting Department: Human Resources

Date: 03/24/2014

Department Address: 96135 Nassau Place, Suite 5
Yulee, Florida 32097

Contact: Tina Keiter (Human Resources Coordinator)

Contact email: tkeiter@nassaucountyfl.com

Department Phone: (904) 491-7332

Department Fax: (904) 321-5797

Product(s)/Service(s) to be purchased (list all specifications and requirements):

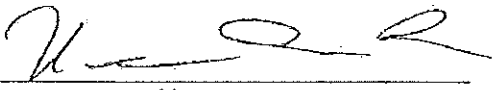
Nassau County is seeking quotes from qualified background service providers to provide services to Nassau County BOCC for the attached services.

Please submit written response by: April 11, 2014
(Date)

To be completed by vendor:

Vendor Name: MAF Background Screening (A DIVISION OF SAREMA)
Address: 1701 Broadway
SAN ANTONIO TEXAS 78215
Phone: 213-892-3963
Fax: 800-226-7785
Contact: Nelson San Pedro
Email: NELSON.SAN PEDRO@MAFScreening.COM

Attached is a written quote from our company, which is valid for 30 days.


Signature

4/7/2014
Date

Comments: _____

Request for Written Quotes

Background Services Requested

1. Criminal County Background
2. Criminal State Background
3. Criminal Federal Background
4. Worker's Compensation

* The above is required for all new hires, on average, 4 a month, based on 6 months of invoice history.

5. Motor Vehicle Check Background

* This is performed on all new hires as well as other circumstances. On average, 5 a month, based on 6 months of invoice history.

6. Educational Background

*These are only required for new hires who fill a position requiring a degree, these are rare, less than 1 a month, based on 6 months of invoice history.

Please quote on the following:

1. We are aware that costs will vary from State to State, thus please quote total prices for all of the above for both Florida and Georgia as those are the most common in our area. (Please break out to include your fee as well as any pass through fees.)
2. Any start up fees, if applicable.
3. The timeframe to receive reports once an order has been placed.

Tina Keiter

From: Nelson San Pedro <nelson.sanpedro@mafscreening.com>
Sent: Tuesday, April 08, 2014 11:46 PM
To: Tina Keiter
Cc: Nelson San Pedro
Subject: MAF Background Screening-Nassau County
Attachments: Scan0004.pdf

Importance: High

Dear Tina,

Here is the additional information.

Please let me know if I can be of assistance.

Thanks!

Tina Keiter

From: Nelson San Pedro <nelson.sanpedro@mascreeing.com>
Sent: Tuesday, April 08, 2014 11:39 PM
To: Tina Keiter
Cc: Nelson San Pedro
Subject: MAF Background Screening-Nassau County
Attachments: NASSAU COUNTY- MAF-SARMA-INTRO 4-2014.doc; MAF MVR State Fees 2014.pdf; MAF Workers Comp Fees 2013.pdf; MAF-County-Criminal-Surcharges 2014.pdf; NASSAU COUNTY-MAF BACKGROUND SCREENING SOLUTIONS 4-2014.doc; WHY SELECT MAF-SARMA 2014.doc; MAF revised training PPT 2014.ppt; SARMA-MAF-SECURITY_POLICY_2014.pdf

Importance: High

Dear Tina,

Thanks so much for the opportunity. I am providing the information requested for your perusal. See attachments.

MAF a division of Sarma has over 80 years in dealing with confidential information. Sarma is currently an agent of Trans Union National Consumer Bureau. This gives us information credibility. MAF has no contracts and or monthly minimum.

Currently we assist the following government agencies in Florida. See below.

1. City of Pompano
 2. Miami Dade Police
 3. City of Deerfield
 4. The Villages
 5. Delray Beach
 6. FDLE
 7. Hernando Sheriff
- Many more!

I would like the opportunity to address this information further.

Please let me know if I can be of assistance.

Thanks!

Nelson San Pedro

MAF Background Screening

Phone: (813) 892-3963

Fax: (813) 283-4964

MAF's Operation Center

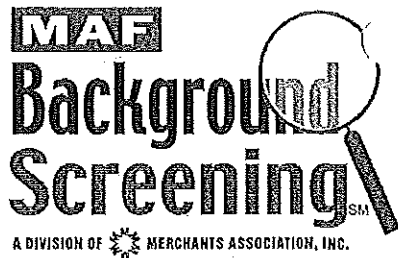
800-226-4483





Check us out on you tube!

MAF Background Screening a division of Sarma.



April 8, 2014

Nassau County

Dear Mrs. Tina Keiter,

We appreciate your interest in our background screening services. MAF is committed to providing your associates with detailed, timely and accurate information.

MAF Background Screening has been providing background screening services to customers since 1984. MAF Background Screening is wholly owned by the Merchants Association of Florida, a not for profit company, that has been conducting business in Florida and Texas since 1900's. In the late 70's MAF/SARMA became part of the Trans Union National Credit Reporting System. MAF/SARMA serviced and maintained the Trans Union National consumer credit information in the State of Florida/Texas for over 30 years. MAF is a consumer reporting agency; therefore customers must follow the new guidelines of Fair Credit Reporting Act (FCRA). All background checks are done with the complete knowledge of the applicant.

MAF-SARMA Background Screening is a full service screening company offering an array of products and services nationwide. Customers can obtain all MAF-SARMA products via the web or outsource the entire screening process to MAF-SARMA. In outsourcing, MAF-SARMA will review the applicants according to your requirements and separate those applicants that meet and don't meet your criteria. The following are some of the MAF-SARMA advantages:

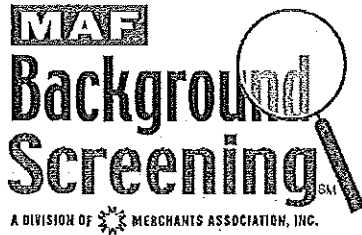
- Operations Center - a live customer representative will handle any questions from 8:30am to 5:00pm (EST-CST)
- Account Executive representation
- No contracts and or monthly minimum
- Secured website available to order and retrieve reports a la carte
- International criminal reports available
- Drug Free workplace/drug testing nationwide
- Offices in the east coast-Tampa and west coast-San Antonio.

Please review all the attached information, and feel free to contact me at anytime if you have any questions. I look forward to hearing from you soon. Thank you for your time and consideration

Sincerely,
Nelson San Pedro
MAF Background Screening a division of Sarma
National Account Executive
Tel.800-226-7757ext.7404
Email: nelson.sanpedro@mafscreening.com

**Workers
Compensation
Information Available**

STATE	INFORMATION	Add'l State Fee
Alaska	State Form with signed release. No ETA	None
Arkansas	W/signed release. Will mail back	\$5.00
Arizona	w/signed release + state form. TAT 7-10 days	\$2.50
California	24-48 Hours.	None
Colorado	Signed & notarized form; TAT 48 hours from receipt of request.	\$1.00
Connecticut	Form must state conditional job offer. TAT 7-14 days	None
Washington DC	24-48 Hours.	None
Florida	24-48 Hours.	None
Iowa	Approximate injury date. TAT 3-5 days	\$6.00
Idaho	Must use state form. 5 year search on work history. TAT 5-7 days	None
Illinois	24-48 Hours.	None
Indiana	w/signed release. 7-10 days TAT	None
Kansas	24-48 Hours.	None
Kentucky	w/signed release TAT 7-10 Days	None
Louisiana	w/signed release. TAT is 3 days.	None
Massachusetts	W/signed release. 10 day TAT	\$5.00
Maryland	24-48 Hours.	None
Minnesota	State form to be signed by the applicant. TAT is 30 days.	None
Missouri	Mail request on state form. TAT 3-15 days	\$5.00
Mississippi	24-48 Hours.	None
Nebraska	24-48 Hours.	\$5.00
New Hampshire	TAT 1 Week	None
New Jersey	TAT 7-10 days state form	.75/page
N. Dakota	24-48 Hours.	None
Ohio	W/signed release form. 3-5 business days	None
Oklahoma	Mail OK state form signed by applicant. TAT 3-5 days.	\$1.00
Pennsylvania	w/signed release must say Xpedite. No TAT	None
South Carolina	Signed release. TAT 3-5 days.	\$10.00
South Dakota	Signed release. TAT is 2-6 days.	\$20.00
Tennessee	TAT 24-48 hours.	\$10.00
Utah	Mail notarized release form. TAT 8-12 days.	\$15.00
Virginia	24-48 Hours. If claim, send notarized form	\$10.00
Vermont	Fax job offer w/signed release. 2-4 days.	None
Washington	w/signed release. TAT is 5-6 days, up to 30 days.	None



EMPLOYMENT SCREENING PRODUCTS AND PRICING NASSAU COUNTY

SSN MATCH/TRACE

Subject verification product based on input name, address and SSN. SSN MATCH returns name, address (current and previous) on subject(s) matching the input name, address and SSN. SSN MATCH also performs an additional search in which input name, SSN and date of birth are matched against public record and commercially available data sources.

Turnaround: Instant
Pricing: \$3.00

TRANS UNION EMPLOYMENT CREDIT REPORT

MAF BACKGROUND SCREENING provides a complete Trans Union credit report from anywhere in the U.S. that satisfies all of the Fair Credit reporting Act compliance for the employer.

Turnaround: Instant
Pricing: \$6.85
\$80 onetime fee for an onsite inspection may apply.

COUNTY CRIMINAL

Search directly and up to date to a county anywhere within the Continental United States and Puerto Rico. The actual county or city name is required in order to obtain this report.

Turnaround: Average is 48 hours
Pricing: \$8.00
* County fees may apply.

FEDERAL CRIMINAL SEARCH

Violations of Federal law are recorded in US Federal District Courts. The number of districts in each state varies, but each state has at least one. While there are fewer violations of Federal laws, they generally involve very serious offenses such as embezzlement, robbery, drug trafficking and kidnapping. Records can be searched by name only and criminal background checks may reveal records, which require further research to confirm the identity of the parties involved.

Turnaround: Instant
Pricing: \$8.00

STATE CRIMINAL REPOSITORY CHECKS

All states have a central repository (database) they use to track known criminals. These state repository criminal record databases are made available to the public by some states but not all. The counties as well as police and other state law enforcement agencies submit criminal records to state's repository criminal record database.

Turnaround: Instant
Pricing: \$5.00
* State fees may apply

7-YEAR CRIMINAL NATIONWIDE SEARCH (TOP SEARCH)

- *SSN Search determines addresses of applicant for last 7 yrs.
- *County criminal search in each county of residence. (Unlimited county search)
- *Multi State Criminal Database search based on Name and Date of Birth.
- *FCRA Compliance Report
- *Includes OFAC and other Terrorist lists
- * Sexual Predator Registry (45 plus states including Florida and DC)
- * **Federal Criminal Record Search included**

Turnaround: 3 to 5 working days on county searches
Price: \$30.00*
Most of the reports come back instant.
County fees may apply.

MOTOR VEHICLE REPORT

Individual driving histories are available from most states throughout the Continental United States. These searches are a complete chronological history of driver's license issuance, restrictions, tickets, suspensions, status, and points accessed.

Turnaround: Instant in most States
Pricing: \$3.00*
* Plus any state fees.

EMPLOYMENT/EDUCATION OR LICENSE VERIFICATION

Education-

MAF will verify with the school regarding claimed education degrees and/or dates of attendance.

Employment- MAF will conduct a verification of claimed previous employment, verification of dates of employment, position held, reason for departure and rehire status, any general comments.

License - We can do license verifications upon request.

Turnaround: 3 Business Days
Pricing: \$9.00
*Per each Employer, license or Degree/University
* Additional fees may apply when using a third party clearing house.

DRUG TESTING

Full line of drug testing is available from our strategic partner including the standard 5 panel urine test. Also available is customized urine, blood and hair testing. With thousands of sites nationally, this can be both convenient and easy for you and your applicant.

Turnaround: Depending upon applicant and type of test
Standard 5 Panel Pricing: \$30.00 via Labcorp or Quest collection sites.
Onsite collection and Drug Free Workplace available upon request!

ADVERSE ACTION SERVICES

Notify your applicant when you intend to deny employment by using some assistance from MAF. Follow the FCRA guideline by doing the following;

- *MAF will mail an official Pre-Adverse Action letter to the applicant within 24 hours of our notification.
- *We will supply the individual with a complete copy of the background screening report along with a copy of the summary of Your Rights, as outlined in the FCRA. Include all necessary contact names and numbers required by law.
- *MAF will handle all inquiries or disputes from the applicant at no additional charge.
- *We will mail the required Adverse Action letter 5 days after the pre adverse letter.

Turnaround: Instant
Pricing: \$12.00 per request/applicant

WORKERS' COMPENSATION

This report identifies a history of claims to avoid habitual claims or to properly channel assignments involving physical labor. Not available in all states. To be included, the claim must have been reported to and recorded with the state Division of Workers' Compensation. This is a post hire service only.

Turnaround: 24 to 48 hrs on results.
Pricing: \$10.00
* Additional fees may apply on other states.

FLORIDA DRIVERS LICENSE MONITORING

We can now monitor driver's reports monthly and advise you once a license status change occurs; i.e. tickets, points suspension, etc. Know when a problem is developing with a driver on a monthly basis rather than once a year. We can save you time and money instead of unnecessarily requesting MVR reports. We will provide a copy of the MVR only on those drivers whose individual record displays adverse information (hits), so the circumstances can be identified and you will have a copy for your records. Many States now available!

Pricing Per Month	\$1.00
Pricing Per Quarter	\$1.50
Pricing Simi Annual	\$2.60
MVR/Hits	\$5.00 plus state fees

MAF Background ScreeningSM

Driving Records - Available States, State Fees and Turnaround Times

State	Years Reported	Instant Access	MVR State Fee	Connection Fee	Request Cut off	Expected Turnaround
Alabama	3	Yes	\$8.25	None	None	Instant
Alaska	-	No	\$10.00	\$1.00	5:00 PM EST	In Excess of 7 Business Days
Arizona	39 months	Yes	\$6.00	None	None	Instant
Arizona	5 certified	Yes	\$8.00	None	None	Instant
Arkansas Driver Check	Status	Yes	\$2.00	None	None	Instant
Arkansas (Insurance)	3	Yes	\$8.50	None	None	Instant
Arkansas Standard	3	Yes	\$11.50	None	None	Instant
California	-	Yes	\$2.00	None	None	Instant
Colorado	7	Yes	\$2.20	None	None	Instant
CDLIS	-	Yes	\$1.85	None	None	Instant
Connecticut	-	Yes	\$15.00	None	None	Instant
Delaware	3	Yes	\$15.00	None	None	Instant
District of Columbia (D.C.)	-	Yes	\$13.00	None	None	Instant
Florida	3	Yes	\$8.10	None	None	Instant
Florida	7	Yes	\$10.10	None	None	Instant
Georgia	3	Yes	\$6.00	None	None	Instant
Georgia	7	Yes	\$8.00	None	None	Instant
Hawaii	7	No	\$23.00	None	5:00 PM EST	9:00 AM EST
Idaho	3	Yes	\$9.00	None	None	Instant
Illinois	-	Yes	\$12.00	None	None	Instant
Indiana	10	Yes	\$7.50	None	None	Instant
Iowa	-	Yes	\$8.50	None	None	Instant
Kansas	-	Yes	\$8.70	None	None	Instant
Kentucky	3	Yes	\$5.00	None	None	Instant
Louisiana	3	Yes	\$6.00	None	None	Instant
Maine	3	Yes	\$7.00	None	None	Instant
Maryland	3	Yes	\$12.00	None	None	Instant
Massachusetts	-	Yes	\$8.00	None	None	Instant
Michigan	5	Yes	\$8.00	None	None	Instant
Minnesota	5	Yes	\$5.00	None	None	Instant
Mississippi	3	Yes	\$14.00	None	None	Instant
Missouri	-	Yes	\$5.80	None	None	Instant
Montana	3	Yes	\$7.25	None	None	Instant
Nebraska	5	Yes	\$3.00	None	None	Instant
Nevada	3	Yes	\$7.00	None	None	Instant
New Hampshire	5	Yes	\$12.00	\$1.00	None	Instant
New Jersey	5	Yes	\$12.00	None	None	Instant
New Mexico	3	Yes	\$6.50	None	None	Instant
New York	5	Yes	\$7.00	None	None	Instant
North Carolina	3/7	Yes	\$8.00	None	None	Instant
North Dakota	3	Yes	\$3.00	None	None	Instant
Ohio	3	Yes	\$5.00	None	None	Instant
Oklahoma	3	Yes	\$27.50	None	None	Instant
Oregon	-	No	\$9.63	\$1.00	5:00 PM EST	6:00 PM EST 2nd Business Day
Oregon	-	Yes	\$9.68	None	None	Instant

(Insurance)						
Pennsylvania	10	No	\$5.00	\$3.00	4:30 PM EST	5 Business Days
Pennsylvania (Insurance)	3	Yes	\$5.00	None	None	Next Business Day.
Rhode Island	3	Yes	\$20.00	None	None	Instant
South Carolina	3/10	Yes	\$7.25	None	None	Instant
South Dakota	3	Yes	\$5.00	None	None	Instant
Tennessee	3	Yes	\$7.00	None	None	Instant
Texas	3	Yes	\$6.50	None	None	Instant
Texas CDL Only	5	Yes	\$7.50	None	None	Instant
Utah	-	Yes	\$9.00	None	None	Instant
Vermont	3	Yes	\$16.00	\$1.00	None	Instant
Virginia 5/7 Yr	-	Yes	\$7.00	None	None	Instant
Washington Driver Check	Status	Yes	\$1.50	None	None	Instant
Washington	-	Yes	\$13.00	None	None	Instant
West Virginia	7	Yes	\$9.00	None	None	Instant
Wisconsin	-	Yes	\$7.00	None	None	Instant
Wyoming	-	Yes	\$5.00	None	None	Instant
Wyoming (CDL Only)	10	Yes	\$5.00	None	None	Instant

Report turnaround is based on past experience but is subject to change by State Motor Vehicle Departments, and delays due to communication and/or processing times.



COUNTY CRIMINAL SURCHARGES

STATE	COUNTY	Surcharge
MICHIGAN (cont.)	Gogebic	\$50.00
	Grand Travers	\$10.00
	Hillsdale	\$20.00
	Houghton	\$40.00
	Huron	\$10.00
	Ionia	\$8.00
	Iosco	\$20.00
	Iron	\$25.00
	Jackson	\$5.00
	Kalkaska	\$5.00
	Kent	\$6.00
	Keweenaw	\$20.00
	Lake	\$5.00
	Lapeer	\$5.00
	Lenawee	\$10.00
	Mackinac	\$20.00
	Manistee	\$6.00
	Marquette	\$15.00
	Mason	\$5.00
	Mecosta	\$10.00
	Menominee	\$12.00
	Midland	\$10.00
	Missaukee	\$15.00
	Montcalm	\$17.00
	Montmorency	\$10.00
	Oceana	\$10.00
	Ogemaw	\$5.00
	Ontonagon	\$10.00
	Osceola	\$10.00
	Oscoda	\$20.00
Otsego	\$6.00	
Ottawa	\$3.00	
Presque Isle	\$5.00	
Sanilac	\$17.00	
Schoolcraft	\$20.00	
Shiawassee	\$10.00	
Tuscola	\$10.00	
Van Buren	\$7.00	
Wexford	\$5.00	

STATE	COUNTY	Surcharge
MISSOURI	All Counties	\$10.00
MISSISSIPPI	George	\$1.00
MONTANA	All Counties	\$13.00
	Beaverhead	\$10.00
	Big Horn	\$25.00
	Blaine	\$14.00
	Carter	\$14.00
	Cascade	\$10.00
	Chouteau	\$14.00
	Custer	\$25.00
	Daniels	\$14.00
	Dawson	\$10.00
	Deer Lodge	\$5.00
	Fallon	\$39.00
	Fergus	\$10.00
	Gallatin	\$25.00
	Garfield	\$14.00
	Glacier	\$28.00
	Golden Valley	\$25.00
	Granite	\$7.00
	Jefferson	\$20.00
	Judith Basin	\$14.00
	Lake	\$10.00
	Lewis And Clark	\$28.00
	Liberty	\$17.00
	Lincoln	\$6.00
	Madison	\$14.00
	Mccone	\$25.00
	Meagher	\$14.00
	Mineral	\$25.00
	Missoula	\$10.00
	Musselshell	\$28.00
Park	\$39.00	
Petroleum	\$14.00	
Phillips	\$14.00	
Pondera	\$4.00	
Powder River	\$25.00	
Powell	\$25.00	
Prairie	\$14.00	



COUNTY CRIMINAL SURCHARGES

STATE	COUNTY	Surcharge
MONTANA (cont.)	Ravalli	\$14.00
	Richland	\$25.00
	Roosevelt	\$14.00
	Rosebud	\$5.00
	Sanders	\$25.00
	Sheridan	\$14.00
	Stillwater	\$14.00
	Sweet Grass	\$7.00
	Teton	\$14.00
	Toole	\$31.00
	Treasure	\$25.00
	Valley	\$14.00
	Wheatland	\$14.00
	Wibaux	\$14.00
NORTH DAKOTA	All Counties	\$10.00
NEW HAMPSHIRE	All Counties	\$2.00
NEW JERSEY	Hillsborough	\$20.00
	Bergen	\$3.00
	Essex	\$3.00
	Hunterdon	\$6.00
	Passaic	\$5.00
NEVADA	Warren	\$6.00
	All Counties	\$7.00
	Douglas	\$14.00
	Lyon	\$14.00
NEW YORK	White Pine	\$14.00
	Albany	\$68.00
	Bronx	\$68.00
	Cayuga	\$68.00
	Chemung	\$20.00
	Cortland	\$68.00
	Greene	\$18.00
	Hamilton	\$68.00
	Kings	\$68.00
	Lewis	\$10.00
	Madison	\$15.00
	Montgomery	\$68.00
	Nassau	\$68.00
	New York	\$68.00

STATE	COUNTY	Surcharge	
NEW YORK (cont.)	Orleans	\$68.00	
	Oswego	\$5.00	
	Queens	\$68.00	
	Rensselaer	\$20.00	
	Richmond	\$68.00	
	Schenectady	\$5.00	
	Schuyler	\$5.00	
	Steuben	\$20.00	
	Tompkins	\$20.00	
	Wyoming	\$5.00	
OHIO	All Counties	\$8.00	
OKLAHOMA	All Counties	\$15.00	
PENNSYLVANIA	Cambria	\$3.00	
	Cumberland	\$3.00	
	Delaware	\$10.00	
	Indiana	\$5.00	
	Luzerne	\$0.00	
PUERTO RICO	All Counties	\$15.00	
SOUTH DAKOTA	All Counties	\$20.00	
TENNESSEE	Carroll	\$5.00	
	Cocke	\$3.00	
	Davidson	\$20.00	
	Hamilton	\$10.00	
	Humphreys	\$7.00	
	Knox	\$10.00	
	Scott	\$10.00	
	Shelby	\$5.00	
	VIRGIN ISLAND	All Counties	\$40.00
	VERMONT	All Counties	\$30.00
WEST VIRGINIA	Brooke	\$5.00	
	Hancock	\$5.00	
WYOMING	All Counties	\$20.00	



COUNTY CRIMINAL SURCHARGES

STATE	COUNTY	Surcharge
CALIFORNIA	Alpine	\$5.00
	Amador	\$5.00
	Colusa	\$5.00
	Contra Costa	\$5.00
	Del Norte	\$15.00
	El Dorado	\$5.00
	Glenn	\$15.00
	Humboldt	\$15.00
	Imperial	\$15.00
	Inyo	\$15.00
	Kern	\$5.00
	Lake	\$5.00
	Lassen	\$5.00
	Los Angeles	\$5.00
	Mariposa	\$15.00
	Mendocino	\$15.00
	Modoc	\$5.00
	Mono	\$5.00
	Monterey	\$0.00
	Placer	\$5.00
Plumas	\$5.00	
San Benito	\$5.00	
Santa Cruz	\$5.00	
Sierra	\$15.00	
Tehama	\$5.00	
Trinity	\$5.00	
Yolo	\$5.00	
COLORADO	Boulder	\$0.75
	Denver	\$0.75
	El Paso	\$0.75
FLORIDA	Baker	\$10.50
	Bradford	\$2.00
	Gadsden	\$2.00
	Gilchrist	\$2.00
	Glades	\$2.00
	Gulf	\$2.00
	Hendry	\$10.50
	Jefferson	\$14.00

STATE	COUNTY	Surcharge
FLORIDA (cont.)	Madison	\$14.00
	Nassau	\$14.00
	Okeechobee	\$7.00
	Sumter	\$2.00
	Taylor	\$2.00
	Wakulla	\$14.00
	Walton	\$2.00
	Washington	\$2.00
	GUAM	All Counties
ILLINOIS	Saint Clair	\$5.00
KANSAS	Wyandotte	\$1.00
KENTUCKY	Anderson	\$15.00
	Jackson	\$15.00
LOUISIANA	Grant	\$5.00
	Orleans	\$10.00
	Red River	\$10.00
MAINE	All Counties	\$30.00
MICHIGAN	Alcona	\$20.00
	Alger	\$15.00
	Allegan	\$0.00
	Alpena	\$15.00
	Antrim	\$10.00
	Arenac	\$15.00
	Baraga	\$15.00
	Barry	\$10.00
	Benzie	\$3.00
	Berrien	\$10.00
	Branch	\$10.00
	Calhoun	\$0.00
	Cass	\$20.00
	Cheboygan	\$0.00
	Chippewa	\$5.00
	Clare	\$16.00
	Crawford	\$5.00
	Delta	\$30.00
Dickinson	\$20.00	
Emmet	\$10.00	
Genesee	\$15.00	



Why Select MAF-SARMA Background Screening

It is important for employers to hire professionals for background screening. A quality background screening service is not the same as a database miner whose limited resources deliver little for the dollar. A professional background screener performs a much broader service for employers who must depend on solid, up-to-date prescreening. Which company you select when outsourcing your screening efforts is important because most businesses are concerned about the cost than the price of a "background check". If you are spending the time, effort and dollars you need not waste them on the wrong search. Outsourcing this background screening core HR function to an established professional background screening company will save you and your entire staff valuable administrative time, and money. Then there is the issue of legal compliance. Background Screening falls under the jurisdiction of the Federal Trade Commission, and is governed by the Fair Credit Reporting Act. A violation of this act can result of an employer defending themselves against a law suite. Make sure you and the background screening company is following the Fair Credit Reporting Act.

In Business over 90 years

Our roots started in the credit industry in the early 1900's as the Credit Bureau of Greater Tampa and San Antonio/Texas and expanded to include many different data reporting services, including national background-screening services

Owned by our customers

We were chartered in the early 1900's as an association of local businesses to support each other by sharing information and assisting each other in making good business decisions. That charter is still in effect, so is our original goal. We are owned by and for those we serve.

Certified by industry in Fair Credit Reporting Act

Each of our customer service personnel has passed the industry testing program to become certified in the Fair Credit Reporting Act. Our years of credit bureau experience provide the industry expertise needed to deal with disputes and applicant's problems. Many times avoiding potential problems with disgruntled applicants

Customize products and services to meet individual business needs.

One size does not fit all, even within the same company. Depending on the position being filled to the specific duties within a position each require the flexibility of products and services to answer the question, is this a good hire. The ability to have a full range of services to fit the multiple variations of needs makes a full service company like MAF Background Screening stand above the others.

Customer Service

Our customer support is in our offices are located in Tampa Florida and San Antonio Texas. Our staff is fully trained in the requirements to fulfill the needs of our customers. Our live phone support is available during working hours; we actually want to answer your question in person.

Highly Secured Internet Access

Our Internet based system has state of the art capability and is continually improved to meet the ever changing needs of our client base. Our system security is based on the most up-to-date security systems and provides protection unsurpassed in the industry. In addition, we are compliant with the new HR Standard interface for data transfer between applications.

Extensive history in data management

The credit reporting industry has been on the leading edge of consumer laws, data gathering and automated technology. The implementation of this knowledge and experience to background screening was natural for our company.

\$5,000,000 error and omissions insurance

We carry \$5,000,000 of error and omissions insurance because it is prudent to do so. We carried this insurance as a credit bureau and continue to provide protection to our customers as one of the premier background screening company's in the industry.



Sarima Comprehensive Security Policy
Revision 2.1

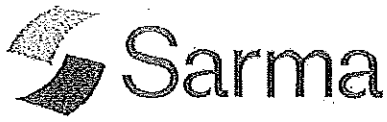


Table of Contents

- Sarman Comprehensive Security Policy..... 1
- Table of Contents 2
- Introduction 4
 - Violations and Discipline 4
 - Administration 4
- Statement of Responsibility 5
 - Management responsibilities 5
 - Information Systems Department responsibilities 5
- Confidential Information 6
 - Employee responsibilities 7
- Workstation Policy 9
 - Purpose 9
 - Scope 9
 - Policy 9
 - Enforcement 10
 - Definitions 10
- Clean Desk Policy 11
 - Purpose..... 11
 - Responsibility..... 11
 - Scope 11
 - Action 11
 - Enforcement 11
- The Internet and E-mail..... 13
 - Policy 13
 - Security Measures 13
 - Downloads..... 13
 - Acceptable use 13
 - Unacceptable use 13
 - Employee responsibilities 14
 - Ownership 15
- VPN Access, Web Based E-mail, and Sarman Issued Hardware..... 16
 - Employee responsibilities 16
- Security Awareness Program 18
 - Documentation 18
- Wireless Access 19
 - Rogue Wireless 19
- Vulnerability Scanning Procedures..... 20
 - Frequency..... 20
 - Process..... 20
- Copyrights and License Agreements 21
 - Legal reference 21
 - Scope 21
 - Information Systems Department responsibilities 21
 - Employee responsibilities 21
 - Civil penalties 21
 - Criminal penalties 22



Encryption Policy23
 Purpose..... 23
 Scope 23
 Policy 23
 Laptops and Desktops 23
 PDAs and Cell phones 23
 File Servers 23
 Archive Data..... 23
 Keys and Encryption Standards..... 23
 Loss and Theft..... 24
 Enforcement 24
 Definitions 24
Sarma Document Retention and Destruction Policy25
 Document Retention 25
 Corporate Records..... 25
 Electronic Documents and Records 27
 Emergency Planning..... 27
 Document Destruction 27
 Compliance 28
Electronic Device Removal Procedures.....29
 Electronic Storage Device Definition 29
 Scenario Definitions 29
 Storage Preparation Procedures 29
 Disposal of Nonstorage Related Electronic Devices 30
Access Codes and Passwords31
 Information Systems Department responsibilities 31
 Employee responsibilities 31
 Human resources responsibility 31
Physical Security32
 Employee responsibilities 32
Red Flags34
Responding to Red Flags37
Antivirus and Spyware Policy39
 Information Systems Department responsibilities 39
 Employee responsibilities 39
EXHIBIT A: Suspicious File Extensions41
Revision History43
Procedure.....46
Signature46



Introduction

The following policies are a compilation of both physical and electronic guidelines for Sarma. The premise is based on the protection of information and assets that are entrusted by Sarma to its employees that constitutes company, client, and consumer Confidential Information. The most recent approved copy of this policy will always be available at our Intranet website www.sarmazine.com. This policy will be reviewed annually and reapproved or adjusted to meet ever changing security needs. Access to any Confidential Information facing technology requires explicit approval based on job description or vendor related coordination with Sarma. This includes but is not limited to: remote access, removable media, laptops, cell phones with Sarma network access, email, or Internet access. The purpose of this group of policies and directives has been established in order to:

1. Protect the investment related to assets and information.
2. Safeguard the information notated as "Confidential" and defined herein.
3. Reduce business and legal risk.
4. Protect the good name of the company.

Violations and Discipline

Employees are expected to abide by all aspects of Sarma's policies regarding electronic and physical information as well as the use of Sarma's electronic systems related to these information sources. Failure to abide with the terms of this group of policies (or any other related Sarma policy) will result in disciplinary action, up to and including termination depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

Administration

The Technology Manager and Human Resources Manager are responsible for the administration of this group of policies. Policies herein will be reviewed and updated on a periodic basis and will be disseminated to staff for validation of changes. Signed confirmation of this policy is due by each employee annually.

Statement of Responsibility

General responsibilities pertaining to this policy are set forth in this section. The subsequent sections list additional specific responsibilities.

Management responsibilities

Management and supervisors must:

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

Information Systems Department responsibilities

The Information Systems Department must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.
3. Purchase and implement all necessary hardware and software to verify that this policy is maintained at a minimal hindrance to other employees work.
4. Monitor and investigate any possible noncompliance within the company as necessary
5. Monitor the policies and actions to implement the policy to verify that it does not hinder any valid work process performed at Sarma.

Employee Responsibilities

Employees must:

1. Read, understand, and agree to the policies that Sarma sets forth in this document concerning information security
2. Take all necessary action to comply with this policy
3. Notify management of any violation of this policy that they are aware of or if equipment is needed to comply.



Confidential Information

Confidential Information may include, by way of example, financial statements, forecasts, data, know-how, client information, "sensitive consumer information," credit information, processes, designs, sketches, schematics, photographs, plans, drawings, specifications, samples, reports, customer and distributor names, pricing information, computer codes, screen shots, forms, information about, or received from, Sarma's current, former and prospective customers marketing information and ideas which are either confidential, proprietary or otherwise not generally available to the public items, which explicitly belong to Sarma or any customer, client, or partner of Sarma.

Sarma personnel are encouraged to use common sense judgment in securing the company's "Confidential Information" to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor/manager. Confidential Information should be masked when displayed unless a legitimate business need exists for Sarma personnel to view the full Confidential Information. Known employee groups that need full access to Confidential Information are accounting, collections administration, mortgage, information technology and certain collector teams.

Sensitive consumer information includes the following items whether stored in electronic or printed format:

Personal Information (also known as Personally Identifiable Information (PII)) - Sensitive information consists of personal information including, but not limited to:

1. Credit Card Information, including any of the following:
 - a. Credit Card Number (in part or whole) otherwise known as the primary account number (PAN)
 - b. Credit Card Expiration Date
 - c. Credit Card CV2 Code
 - d. Cardholder Name
 - e. Cardholder Address
2. Tax Identification Numbers, including:
 - a. Social Security Number
 - b. Social Insurance Number
 - c. Business Identification Number
 - d. Employer Identification Numbers
3. Payroll information, including, among other information:



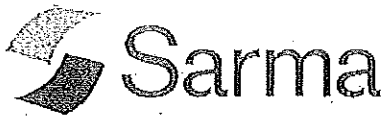
- a. Paychecks
- b. Pay stubs
- c. Pay rates
4. Cafeteria Plan Check Requests and associated paperwork
5. Medical Information for any Employees, Debtors, or Customers, including but not limited to:
 - a. Protected health information (PHI), under the US Health Insurance Portability and Accountability Act (HIPAA), is any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history, Doctor's name, condition, etc.
 - b. Insurance claims
 - c. Prescriptions
 - d. Any other related personal medical information
6. Other Personal Information belonging to Customers, Debtors, Employees and Contractors, examples of which include:
 - a. Date of Birth
 - b. Address
 - c. Phone Numbers
 - d. Maiden Name
 - e. Names
 - f. Customer Number

Credit card tracking data such as the CVC code, PIN, etc may not be stored in any form locally. This information must be shredded in a secure shred bin or securely deleted after initial use immediately.

Employee responsibilities

An employee who deals with any confidential information used by Sarma must comply with the following standards:

1. Information which is considered private or confidential shall not be transferred through the Internet without a business reason directly related to Sarma. No other method of transfer of business related information is allowed other than via a Sarma domain based e-mail account. This would include file transfers via instant messaging, FTP, NNTP, floppy disk, CD ROM, personal e-mail account, or any



other electronic file transfer device without the written permission of a manager or standards related to the individual's job description or duties.

2. Information which is considered private or company confidential shall not be transferred through the Internet without taking precaution to insure the information is properly protected. "Protection" in this context means that information shall not be disclosed to anyone other than its intended recipient. All protection schemes utilized such as encryption shall be reviewed and approved in advance by the Information Systems Department, if this added level of security is deemed necessary by management.
3. Confidential information that is not in use must either be placed in a company approved shred bin for certified disposal or locked in a secure cabinet or drawer for later use (Review the "Clean Desk Policy" for more details). All Confidential Information must be destroyed and/or retained based on the Sarma Retention and Destruction Policy.
4. All Sarma related work in electronic format is to be stored on the related user's home directory so that it is secure and backed up daily. If applicable, this information should be placed in a separate encryption store based on the type of business or department.

Workstation Policy

Purpose

The purpose of this policy is to provide guidance for workstation security in order to ensure the security of "Confidential Information" on the workstation and "Confidential Information" the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

Scope

This policy applies to all Sarma employees, contractors, workforce members, vendors and agents with a Sarma-owned workstation connected to the Sarma network.

Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of "Confidential Information" and that access to "Confidential Information" is restricted to authorized users.

- Workforce members using workstations shall consider the sensitivity of "Confidential Information" that may be accessed and minimize the possibility of unauthorized access.
- Sarma will implement physical and technical safeguards for all workstations that access "Confidential Information" to restrict access to authorized users. Appropriate measures include:
 - Restricting physical access to workstations to only authorized personnel.
 - Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
 - Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. Automated locks on workstations occur at fifteen (15) minutes of idle time (this limitation also applies to all remote access). It is still recommended to manually lock workstations when a user is not present
 - Complying with all applicable password policies and procedures as outlined in the Password Protection Policy. The Information Systems Department will maintain a domain password policy to include, but not be limited to: mandatory password changes every 30 calendar days, password complexity requirements (mixed case, alphanumeric, eight or more characters) and password history limitations (no reuse allowed for past three passwords).
- Ensure workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Store all "Confidential Information" on network servers and not on local workstations.
- Keep food and drink away from workstations in order to avoid accidental spills. All drinks in desk areas must be covered.



- Complying with the Antivirus and Spyware policy
- Ensure that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensure workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents
- All workstations must comply with the Configuration Standard outlined for the department associated with it. In this standard, all approved software and hardware specific items related to the department and business functions will be outlined. Software outside this Configuration Standard must have written preapproval from the manager of that department and the Technology Manager.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Workstations include: laptops, desktops, PDAs, and authorized home workstations accessing the Sarma network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of Sarma

Clean Desk Policy

Purpose

The purpose for this policy is to establish a culture of security and trust for all employees at Sarma. An effective clean desk effort involving the participation and support of all Sarma employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.

The main reasons for a clean desk policy are:

1. A clean desk can produce a positive image when our customers visit the company.
2. It reduces the threat of a security incident as confidential information will be locked away when unattended.
3. Sensitive documents left in the open can be stolen by a malicious entity.

Responsibility

All staff, employees and entities working on behalf of Sarma are subject to this policy

Scope

Employees are expected to follow this policy at all times, however the following times are most critical:

1. At known extended periods away from your desk, such as a lunch break
2. At the end of each working day
3. When in the presence of vendors, visitors, clients, contractors, or other uncredentialed employees.

Action

1. Allocate time in your calendar to clear away your paperwork.
2. Always clear your workspace of all identifiable paperwork that falls under the "Confidential Information" definition.
3. If you are unsure whether a duplicate piece of "Confidential Information" should be kept, throw it out securely.
4. Use the identified, secured and confidential shred bins in various areas around the building for sensitive documents when they are no longer needed.
5. Lock your desk and filing cabinets at the end of the day.
6. If you are in an office, ensure that the door is locked when you are away. If your office does not have a lock, notify the building administrator.
7. Lock away computing devices such as laptops, hard drives or PDA devices when not in use.
8. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked storage area when not in use.

Enforcement



Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



The Internet and E-mail

Policy

Access to the Internet is provided to employees for the benefit of Sarma and its customers. Employees are able to connect to a variety of business information resources around the world. Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the company's interests, the following guidelines have been established for using the Internet and e-mail.

Security Measures

Sarma employs SPAM and web filtering tools to ensure that this policy is followed. Management reserves the right to restrict access to related services to ensure the safety and security of the company, its clients, data under its charge, and its employees.

Downloads

Any file downloaded from the Internet that is not a normal part of a user's job function is not permitted unless specifically authorized in writing by a manager. This includes screen savers, applications, instant messaging tools, any file sharing tool, MP3s, video clips, etc.

Acceptable use

Employees using the Internet are representing Sarma. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

1. Using Web browsers to obtain business information from commercial web sites.
2. Accessing databases for information as needed concerning clients or our clients' customers.
3. Using e-mail for business contacts and potential new business.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, or are harmful to Sarma or its clients. Examples of unacceptable use are:

1. Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
2. Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list, unless that list is a current list of your own clients, or is an approved distribution list in the Sarma Global Address List. A broadcast e-mail to NONclients or potential clients is not acceptable unless previously approved in writing by a manager (i.e. SPAM).



3. The display of any kind of sexually explicit image or document on any Sarman system is a violation of Sarman's policy on sexual harassment. Sexually explicit material may not be accessed, archived, stored, distributed, edited or recorded using Sarman's equipment, network or computing resources. Internet websites that contain profane, obscene and/or sexually explicit language or topics may not be accessed by Sarman employees using Sarman's equipment. The use of profanity, derogatory epithets, innuendo and/or sexual, threatening, abusive or obscene language on Sarman's electronic systems is prohibited.
4. Employees are prohibited from using Sarman's electronic systems or communications to harass or intimidate co-workers, customers or any individual, regardless of whether the recipient of the communication is on or off company premises.
5. Visiting websites that contain illegal items or activity, gambling, violence, hacking, or other types of unacceptable or offensive activities.
6. Users should not develop and/or test remote access capabilities other than those specified in job descriptions or as assigned in projects by Sarman management.
7. Use of personal email accounts (i.e. Comcast, RoadRunner, AT&T, AOL, etc), personal Webmail (i.e. Hotmail, Gmail, etc), chat, social networking, blogs, or other related activities outside of preapproved venues such as Sarman's break room kiosks are prohibited unless it relates to one's job function.
8. Use of services like newsgroups, file sharing, and peer to peer services such as "Torrents" are prohibited in any Sarman environment.
9. Due to constant change in technology, management reserves the right to adjust these restrictions as necessary.

Employee responsibilities.

An employee who uses the Internet or e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable Sarman policies dealing with security and confidentiality of company records.
5. Agree not to download/receive via e-mail any item that has questionable content or attachment(s) or solicit such items from friends, coworkers, or any other outside source. (see Exhibit A)
6. Avoid transmission of confidential information unless necessary to your job function.
7. Use the Sarman provided kiosks for personal use during breaks and lunches.



Ownership

All messages and other items created, sent, or retrieved over the Internet are the property of Sarma. Sarma reserves the right to access the contents of any messages, files or other items sent over its facilities or stored on its property if the company believes, in its sole discretion, that it has a business or legal need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. This type of monitoring can include, but is not solely limited to:

- E-mail content
- Instant messaging
- Chat room sessions
- Web site activity
- Files and images
- Documents
- Other items as deemed necessary



VPN Access, Web Based E-mail, and Sarima Issued Hardware

If you are an authorized user of Sarima's Virtual Private Network (VPN), then you have an added responsibility when it comes to the Internet and e-mail access. If you are issued Sarima owned hardware, you also have added responsibilities.

The VPN allows a user to directly access the Sarima network to use e-mail and other network resources while away from the Sarima physical office. This added feature adds the responsibility to make sure the network is safe from nonSarima employees while this access is active. This is a serious responsibility and is not to be taken lightly.

Remote access through VPN requires two-factor authentication or greater.

Access to any Sarima system by a vendor requires the following limitations:

1. Access must be disabled when not in use
2. Access enabled only when documented need is established
3. Access is monitored at all times
4. Access by approved vendors assumes all security responsibilities of employees (see vendor version of security policy).

Employee responsibilities

All VPN authorized employees and employees with company issued hardware are responsible for the following:

1. When the VPN connection is active, employee must be present with that connection at all times. If employee leaves the computer using the VPN at any time, employee must disconnect the VPN access immediately.
2. Disconnect immediately when employee is finished working with the VPN and close all Sarima related documents.
3. If employee needs to walk away from the connection for any reason, employee must lock the hardware (CTRL+ALT+DEL) so that unauthorized access is not given to a nonSarima employee. (read the "Confidential Information" section to understand the importance of Sarima information security)
4. As an entrusted employee with Sarima hardware outside of the Sarima office, one must never allow a nonSarima employee to access, view, or use the Sarima hardware for any reason. This can include, but is not limited to: checking private e-mail, using applications on the laptop, view or change Sarima information, etc.
5. Do not use the VPN for extended periods for nonproductive use. The VPN has a limited number of live connections. Keep this in mind while you are connected so that all users have the time they need to do their work.



6. When logged into Sarima web based e-mail, do not leave it unattended at any time. Treat it as sensitively as the VPN connection.
7. When logging into web based e-mail via a client's site, be sure to close the browser after you log off. Only a closed browser verifies the web e-mail session termination process.
8. Users must not store on Sarima hardware or home computers any company data that compromises Sarima's information trust and its competitiveness without prior authorization from the Operations Committee and proper security measures, such as encryption and password protection. All data must be stored on the Sarima private network.



Security Awareness Program

All employees are required to attend annual security awareness training. This training may be modified at any time to accommodate security needs over time. This program will include video, online and live interaction with the IS Department to ensure all employees are aware of potential risks related to social engineering, securing Confidential Information, security requirements, etc.

In addition to training on standard security principles, all employees directly involved with credit data or other regulated practices as a part of their job function will be required to pass a relevant certification exam. Current requirements (amended as needed):

- Employees in the credit or credit reseller verticals, FCRA certification and annual renewal is required
- Employees in the collections vertical, FDCPA certification and annual renewal is required.

All employees directly involved with credit data will be required to review and acknowledge the related bureau's reseller policy annually.

Documentation

Human Resources will maintain a signed attendance record of security awareness program attendance and testing, as applicable. The IS Department will maintain the program and its content, which will be updated and administered annually.

Wireless Access

It is Sarman's policy to not maintain a wireless network that is attached to the Sarman network with access to Confidential Information or any other Sarman domain related resource. Any wireless access on Sarman's physical property must be Sarman controlled but outside this internal network, be separately monitored, maintained and filtered. Any wireless network that is attached to the Sarman internal network (as defined as being on the same subnet and/or Windows domain) as internal resources such as Confidential Information will be defined as a "rogue" wireless network

Rogue Wireless

The following procedures are required in relation to rogue wireless network(s):

1. Detection of rogue wireless networks is the responsibility of the IS Department. Detection procedures must be conducted at a minimum of monthly using tools to search for these signals.
2. All wireless access that is identified to have a strong signal in the physical vicinity must be researched.
3. Examples of potential rogue wireless situations include:
 - WLAN cards installed as system components in workstations
 - Unapproved portable wireless devices connected to the Sarman network (i.e. hotspot devices, mifis, etc.
 - Wireless access devices directly connected to an "on network" Ethernet port in the physical facility.
4. If a wireless access point is identified on the network, this will be considered a breach, and must engage an incident response procedure. The wireless access must be disabled, documented and researched immediately.

Vulnerability Scanning Procedures

Vulnerability scanning is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in then enterprise.

Frequency

Sarima will engage in vulnerability scanning of the company's networks at least quarterly. This scan must be repeated if any issues or vulnerabilities are found and must be resolved until a passing scan is achieved.

Scans must also be performed on an ad hoc basis after any major network change such as domain structure, new installation of technology, equipment or similar event.

Process

The procedure for scanning involves engaging a third party resource that will scan the network from the outside. This scan must be performed by an approved, contracted vendor (currently McAfee and Security Metrics). Internal scans also must be performed by the IS Department on the same frequency.

Detection of rogue wireless networks is the responsibility of the IS Department. Detection procedures must be conducted at a minimum of monthly using tools to search for these signals.

All wireless access that is identified to have a strong signal in the physical vicinity must be researched.

Examples of potential rogue wireless situations include:

- WLAN cards installed as system components in workstations
- Unapproved portable wireless devices connected to the Sarima network (i.e. hotspot devices, mifis, etc.
- Wireless access devices directly connected to an "on network" Ethernet port in the physical facility.

If a wireless access point is identified on the network, this will be considered a breach, and must engage an incident response procedure. The wireless access must be disabled, documented and researched immediately.



Copyrights and License Agreements

It is Sarima's policy to comply with all laws regarding intellectual property.

Legal reference

Sarima and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U.S. Code) and all proprietary software license agreements. Noncompliance can expose Sarima and the responsible employee(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by Sarima, licensed to Sarima, or developed using Sarima resources by employees or vendors.

Information Systems Department responsibilities

The Information Systems Department will:

1. Maintain records of software licenses owned by Sarima.
2. Periodically (at least quarterly) scan company computers to verify that only authorized software is installed.
3. Maintain a list of all electronic assets that Sarima owns.
4. Periodically (at least quarterly) verify that computers are being scanned for viruses on a regular basis and that all virus definitions are up to date.

Employee responsibilities

Employees shall not:

1. Install software unless authorized by the Information Systems Department. Only software that is licensed to or owned by Sarima is to be installed on Sarima computers, and must be done by authorized personnel.
2. Copy software unless authorized by the Information Systems Department.
3. No employee may use Sarima facilities/equipment to knowingly download or distribute pirated (stolen) software or data.

Civil penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

1. Liability for damages suffered by the copyright owner
2. Profits that are attributable to the copying
3. Fines up to \$100,000 for each illegal copy



Criminal penalties

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the employee(s) responsible to the following criminal penalties:

1. Fines up to \$250,000 for each illegal copy
2. Jail terms of up to five years



Encryption Policy

Purpose

This document outlines requirements for encrypting data at rest on Sarima devices.

Scope

This policy applies to any mobile device issued by Sarima or used for Sarima business which contains stored data owned by Sarima. It also applies to "Confidential Information" at rest on company file servers and storage devices used for archival (i.e. tape devices)

Policy

All mobile devices containing stored data owned by Sarima must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, PDAs, and cell phones.

Users are expressly forbidden from storing "Confidential Information" on devices that are not issued by Sarima, such as storing Sarima email on a personal cell phone or PDA.

Laptops and Desktops

Laptops and desktops outside the Sarima physical office must employ full disk encryption with an approved software encryption package that is issued and managed by the Information Systems Department. No Sarima "Confidential Information" may exist on a laptop or desktop outside the Sarima physical office in clear text.

PDAs and Cell phones

Any "Confidential Information" stored on a cell phone or PDA must be saved to an encrypted file system using Sarima approved software. Sarima shall also employ remote wipe technology to remotely disable and delete any data stored on a Sarima PDA or cell phone which is reported lost or stolen.

File Servers

"Confidential Information" stored on network file servers will be stored in an encrypted folder which is accessible only to users with express written permission to do so through their job function or management request.

Archive Data

Archived data taken out of the Sarima physical premises will be stored in encrypted form while stored in a secure location off site.

Keys and Encryption Standards



All keys and encryption standards used for encryption and decryption must meet complexity requirements based on current generally accepted business practices.

Loss and Theft

The loss or theft of any mobile device containing "Confidential Information" must be reported immediately.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Clear text	Unencrypted data
Full disk encryption	Technique that encrypts an entire hard drive, including operating system and data
Key	Phrase used to encrypt or decrypt data
PDA	Personal Data Assistant.
Remote wipe	Software that remotely deletes data stored on a mobile device.

S Institute 2006 All Rights Reserved



Sarima Document Retention and Destruction Policy

Purpose

In accordance with the Sarbanes-Oxley Act, which makes it a crime to alter, cover up, falsify, or destroy any document with the intent of impeding or obstructing any official proceeding, this policy provides for the systematic review, retention and destruction of documents received or created by Sarima in connection with the transaction of organization business. This policy covers all records and documents, regardless of physical form, contains guidelines for how long certain documents should be kept and how records should be destroyed. The policy is designed to ensure compliance with federal and state laws and regulations, to eliminate accidental or innocent destruction of records and to facilitate Sarima's operations by promoting efficiency and freeing up valuable storage space.

Document Retention

Sarima follows the document retention procedures outlined below. Documents that are not listed, but are substantially similar to those listed in the schedule will be retained for the appropriate length of time.

Corporate Records

Record Type	Retention Period
Annual Reports to Secretary of State/Attorney General	Permanent
Articles of Incorporation	Permanent
Board Meeting and Board Committee Minutes	Permanent
Board Policies/Resolutions	Permanent
By-laws	Permanent
Construction Documents	Permanent
Fixed Asset Records	2 years
IRS Application for Tax-Exempt Status (Form 1023)	Permanent
IRS Determination Letter	Permanent
Contracts (after expiration)	7 years
Correspondence (general)	3 years
Accounting and Corporate Tax Records	
Annual Audits and Financial Statements	10 years
Financial Statements	10 years
Depreciation Schedules	2 years
General Ledgers	10 years
IRS 990 Tax Returns	Permanent
Business Expense Records	7 years
IRS 1099s	7 years
Journal Entries	7 years



Invoices	7 years
Petty Cash Vouchers	2 years
Cash Receipts	2 years
Credit Card Receipts	2 years
Sales Tax Reports	7 years
Bank Records	
Check Registers	2 years
Bank Deposit Slips	2 years
Bank Statements and Reconciliation	7 years
Electronic Fund Transfer Documents	2 years
Payroll and Employment Tax Records	
Unemployment Tax Records	10 years
Earnings Records	7 years
Accounts Receivable Documentation	2 years
Garnishment Records	7 years
Payroll Tax returns	Permanent
W-2 Statements	Permanent
401K documentation	Permanent
Expired Contracts	7 years
Accounts Payable Invoices	7 years
Other Accounting Documentation	2 years
All Other Payroll Records	10 years
Employee Records	
Employment and Termination Agreements	10 years
Retirement and Pension Plan Documents	Permanent
Records Relating to Promotion, Demotion or Discharge	7 years after termination
Accident Reports	10 years
Worker's Compensation Records	Permanent
Salary Schedules	5 years
Employment Applications	10 years
I-9 Forms	10 years after termination
Time Cards	10 years
Donor Records and Acknowledgement Letters	7 years
Grant Applications and Contracts	5 years after completion
Legal, Insurance and Safety Records	
Appraisals	Permanent
Copyright Registrations	Permanent
Environmental Studies	Permanent
Insurance Policies (after expiration)	2 years



Real Estate Documents	Permanent
Stock and Bond Records	Permanent
Trademark Registrations	Permanent
Leases (after expiration)	2 years
OSHA Documents	10 years
General Contracts	3 years after termination
Collection Accounts	
Closed Accounts – Uncollectable	7 years
Closed Accounts – PIF or SIF	7 years
Closed Accounts – Disputes, Deceased, Bankruptcy, Withdrawn	2 years
Active Accounts	7 years (from date of service)
Original Placement Data From Client	6 months after placement
Mortgage Back Up Documentation	
Faxes and Related Material – Archive (Offline)	3 months
Faxes and Related Material – Purge	2 years

Electronic Documents and Records

Electronic documents will be retained as if they were paper documents. Therefore, any electronic files, including records of donations made online, that fall into one of the document types on the above schedule will be maintained for the appropriate amount of time. Backup and recovery methods will be tested on a regular basis.

Emergency Planning

Sarma's records will be stored in a safe, secure and accessible manner. Documents and financial files that are essential to keeping Sarma operating in an emergency will be duplicated or backed up at least every week and maintained off site.

Document Destruction

Sarma's chief financial officer is responsible for the ongoing process of identifying its records, which have met the required retention period and overseeing their destruction. Destruction of financial and personnel-related documents will be accomplished by shredding through a certified vendor. Electronic records that fall in these categories will be destroyed using methods similar to those outlined in the "Electronic Device Removal Procedures related to electronic storage devices.

Document destruction will be suspended immediately, upon any indication of an official investigation or when a lawsuit is filed or appears imminent. Destruction will be reinstated upon conclusion of the investigation.



Compliance

Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against Sarma and its employees and possible disciplinary action against responsible individuals. The chief financial officer and finance committee chair will periodically review these procedures with legal counsel or the organization's certified public accountant to ensure that they are in compliance with new or revised regulations.

Electronic Device Removal Procedures

Note: *Any electronic devices or media awaiting processing under these procedures must be securely stored (e.g. in a locked closet, server room, office or drawer) and should never be left unattended in a public area.*

Electronic Storage Device Definition

Electronic storage device in this case refers to any type of media that has the capacity to store data, whether temporary or permanent. Examples include but are not limited to: hard drives, USB flash drives, CD ROMS, DVD ROMS, magnetic tapes, floppy disks, random access memory devices, etc.

Scenario Definitions

- 1) Electronic storage devices temporarily leaving Sarman for repair must have their data encrypted or removed following the designated solution in this policy.
- 2) Electronic storage devices permanently leaving Sarman must be disposed of following the designated solution in this policy.

Storage Preparation Procedures

- 1) If the storage component of the electronic storage device is functioning and is scheduled or intended for temporary removal from the network, all data should be either
 - a. Encrypted using a 256-bit or larger key, or
 - b. Removed by software that replaces previously stored data on a drive or disk with a predetermined pattern of meaningless information; a disk "initialization" or "formatting" is insufficient.
- 2) If the purpose of the repair is to recover lost data from an electronic storage device, a vendor confidentiality agreement must be on file for the proposed vendor prior to proceeding.
- 3) If the storage component of the electronic storage device is scheduled or intended for permanent removal from the Sarman network, all data should be processed as follows:
 - i. If the storage component of the electronic storage device is non-functioning, it must be either permanently disabled through dismantling and disabling the plates or other storage media.
 - ii. Degaussed (concept as explained by [Wikipedia](#))
 - iii. Prior to destruction, if applicable, the device will be erased using methods based on the United States Department of Defense



recommendation 5220-22.M from January 1995 by the Information Systems Department. The data will be overwritten seven times. No such media will be allowed to be thrown out or destroyed in any other manner.

- iv. Submitted to a Sarma approved and certified hardware shredding vendor.

Disposal of Nonstorage Related Electronic Devices

Proper disposal of electronic media other than hard drives is authorized, as applicable, in the following order:

- i. Donation
- ii. Recycling vendor
- iii. Legal waste disposal



Access Codes and Passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

Information Systems Department responsibilities

1. The Information Systems Department shall be responsible for the administration of access controls to all company computer systems.
2. The Information Systems Department will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor or manager.
3. The Information Systems Department will maintain a domain password policy to include, but not be limited to: mandatory password changes every 30 calendar days, password complexity requirements (mixed case, alphanumeric, eight or more characters) and password history limitations (no reuse allowed for past three passwords).

Employee responsibilities

Each employee is responsible for the following:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained by others.
3. Should use passwords that will not be easily guessed by others.
4. Should log out or lock a workstation when leaving for an extended period.
5. Passwords will be changed on a regular basis, either by the user, or by the IS department

Human resources responsibility

Human Resources should notify the Information Systems Department promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked or changed immediately. Involuntary terminations must be reported concurrent with the termination.



Physical Security

It is company policy to protect physical premises, computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee responsibilities

The directives below apply to all employees:

1. Unless it is necessary to perform a job function, use of flash drives (aka thumb drives, portable hard drives, USB drives, etc), floppy disks, CD ROMs, DVD ROMs, and any other portable electronic media is expressly prohibited on site. If they are necessary for a job function:
 - i. All portable media must be validated through the Information Systems Department. In some cases, such as flash drives, they must also be registered on the network before they can be deemed usable.
 - ii. Media should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up in a secure area.
 - iii. Media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
2. Storage media, including, but not limited to: hard drives, RAM, floppy disks, back up tapes, CD ROMs, DVD ROMs, and other electronic storage devices used at Sarman for business purposes must be disposed of based on the "Sarman Retention and Destruction Policy."
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the Information Systems Department is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of Sarman issued laptops.
6. Employees shall not take equipment such as computers out of the building without the informed consent of their department manager, in writing. Informed consent means that the manager knows what equipment is leaving, when it is returning, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.



8. Employees shall not be allowed to access the Sarima server room or closed technology closets without prior permission.
9. Closed Caption Television may or will be used to monitor key areas of the company as deemed necessary.
10. Multiple layers of electronic access control may or will be employed to ensure the safety of equipment, data, and personnel.
11. Access to the physical premises is controlled by job function. Entering the building(s) through means, timeframes or entries outside those assigned are prohibited.
12. Controlled access is monitored based on electronic keycard access. One entry per person based on their card is allowed at a time. Knowingly allowing others to enter on a single "swipe" for access is prohibited. This is called "tailgating" and is prohibited.
13. The premises will be monitored by a third party alarm company which handles remote fire and intrusion access. Upon alarm activation, the appropriate authorities will be notified immediately and automatically. Instructions for this situation and relation to the alarm company will be clearly posted near the rear entrance.
14. Any employee that needs to access the physical premises in an "open and close" capacity must have an active security code with the third party security monitoring company. This access is restricted and is issued on a job function basis upon written request from management. When this access is revoked, the building administrator needs to be notified immediately.
15. The IS Department will conduct physical audits of each department to validate best security practices no less than quarterly. Each manager related to the department will be notified of any issues in meeting minimum standards. Manager will be required to address them in writing and return to the IS Department.



Red Flags

The following "Red Flags" are potential indicators of fraud and any time when a "Red Flag," or a situation closely resembling a "Red Flag," is apparent, it should be investigated for verification based on the "Responding to Red Flags" section.

1. Alerts, Notifications or Warnings from a Consumer Reporting Agency
 - a. A fraud or active duty alert is included with a consumer report.
 - b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
 - c. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of this part.
 - d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - i. A recent and significant increase in the volume of inquiries
 - ii. An unusual number of recently established credit relationships
 - iii. A material change in the use of credit, especially with respect to recently established credit relationships
 - iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor
2. Suspicious Documents
 - a. Documents provided for identification appear to have been altered or forged.
 - b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
 - c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
 - d. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
 - e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
3. Suspicious Personal Identifying Information
 - a. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
 - i. The address does not match any address in the consumer report
 - ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File



- b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
 - c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
 - i. The address on an application is the same as the address provided on a fraudulent application
 - ii. The address on an application is the same as the address provided on a fraudulent application
 - d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
 - i. The address on an application is fictitious, a mail drop, or prison
 - ii. The phone number is invalid, or is associated with a pager or answering service
 - e. The SSN provided is the same as that submitted by other persons opening an account or other customers.
 - f. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
 - g. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - h. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
 - i. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
4. Unusual Use of, or Suspicious Activity Related to, the Covered Account
- a. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.
 - b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - i. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry)



- ii. The customer fails to make the first payment or makes an initial payment but no subsequent payments
 - c. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - i. Nonpayment when there is no history of late or missed payments; A material increase in the use of available credit
 - ii. A material change in purchasing or spending patterns
 - iii. A material change in electronic fund transfer patterns in connection with a deposit account
 - iv. A material change in telephone call patterns in connection with a cellular phone account
 - d. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
 - e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
 - f. The financial institution or creditor is notified that the customer is not receiving paper account statements.
 - g. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.
- 5. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor
 - a. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Responding to Red Flags

Once potentially fraudulent activity is detected, it is essential to act quickly as a rapid appropriate response can protect customers and the company from damages and loss.

Response should include:

1. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Take this information and present it to the designated authority for determination.
2. The designated program representative will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
3. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
 - a. Cancel the transaction
 - b. Notify and cooperate with appropriate law enforcement
 - c. Determine extent of liability to company
 - d. Notify actual customer that fraud has been attempted

Periodic Updates to Plan

At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

Periodic reviews will include an assessment of which accounts are covered by the program.

As part of the review, Red Flags may be revised, replaced or eliminated. New Red Flags may also be appropriate.

Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the company and its customers.

Program Administration

- a. Involvement of Senior Management
 - i. The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs and its importance warrants the highest level of attention.
- b. Staff Training
 - i. Staff training shall be conducted for all employees, contractors for whom it is reasonably foreseeable that they may come into contact with accounts or "Confidential Information" which may constitute a risk to the company or its customers.



- ii. Staff members shall continue to receive training as required as changes to the program are made to ensure maximum effectiveness of the program.
- c. Oversight of Service Provider arrangements
 - i. It is the responsibility of the company to ensure that the activities of all Service Providers are conducted in accordance with reasonable policies and procedures designed to detect prevent, and mitigate the risk of identity theft.
 - ii. A Service Provider that maintains its own Identity Theft Prevention Program, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
 - iii. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

Antivirus and Spyware Policy

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs. The original virus may modify the copies, or the copies may modify themselves, as occurs in a metamorphic virus. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive.

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.

It is important to know that:

1. Computer viruses are much easier to prevent than to cure.
2. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Information Systems Department responsibilities

Information Systems Department shall:

1. Install and maintain appropriate antivirus software on all computers. Antivirus definition files must be kept up to date at all times.
2. All critical system and software patches related to the operating system and software in use must be tested and installed within 30 days of release or immediately if related to a critical nature.
3. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.



2. Employees shall not load media that they have received or have brought in on their own unless otherwise authorized.
3. Incoming media must be scanned for viruses before they are used.
4. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the Help Desk.



EXHIBIT A: Suspicious File Extensions

Following is a partial list of file types that should be considered suspicious when received in email and should not be opened unless you requested or expected the attachment:

- ADE - Microsoft Access Project Extension
- ADP - Microsoft Access Project
- BAS - Visual Basic Class Module
- BAT - Batch File
- CHM - Compiled HTML Help File
- CMD - Windows NT Command Script
- COM - MS-DOS Application
- CPL - Control Panel Extension
- CRT - Security Certificate
- DLL - Dynamic Link Library
- DO* - Word Documents and Templates
- EXE - Application
- HLP - Windows Help File
- HTA - HTML Applications
- INF - Setup Information File
- INS - Internet Communication Settings
- ISP - Internet Communication Settings
- JS - JScript File
- JSE - JScript Encoded Script File
- LNK - Shortcut
- MDB - Microsoft Access Application
- MDE - Microsoft Access MDE Database
- MSC - Microsoft Common Console Document
- MSI - Windows Installer Package
- MSP - Windows Installer Patch
- MST - Visual Test Source File
- OCX - ActiveX Objects
- PCD - Photo CD Image
- PIF - Shortcut to MS-DOS Program
- POT - PowerPoint Templates
- PPT - PowerPoint Files
- REG - Registration Entries
- SCR - Screen Saver
- SCT - Windows Script Component
- SHB - Document Shortcut File
- SHS - Shell Scrap Object
- SYS - System Config/Driver



URL - Internet Shortcut (Uniform Resource Locator)
VB - VBScript File
VBE - VBScript Encoded Script File
VBS - VBScript Script File
WSC - Windows Script Component
WSF - Windows Script File
WSH - Windows Scripting Host Settings File
XL* - Excel Files and Templates

* Also included are files without extensions or files with extension names written backwards (i.e. .doc listed as .cod)

Revision History

Revision 1.7 Updates

- Update terminology related to storage media and other technologies
- Added web accessible link to current policy version.
- Added annual review information
- Updated logo and company reference information.
- Added physical security details

Revision 1.8 Updates

- Plan was reviewed and no changes were made.

Revision 1.9 Updates

- Plan was reviewed and no changes were made.

Revision 2.0 Updates

- Various updates were made to comply with PCI DCC V.2.0 requirements:
 - Deleting and Destroying Cardholder Data
 - Policy requiring the most recent version of the information security policy to be published and disseminated to all relevant system users (including vendors, contractors, and business partners).
 - Policy requiring the information security policy to be reviewed at least annually to keep it up to date with changes to the business objectives or risk environment.
 - Employee Assigned Technology Documentation
 - Policy requiring explicit approval by authorized parties prior to using any employee assigned technology in the cardholder environment e.g. remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage).

- Policy requiring any technology used to be authenticated with a user ID and password or other authentication item (for example, token).
- Policy stating the acceptable uses of each allowed employee assigned technology.
- Policy restricting activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.
- Formal Security Responsibility Assignment:
 - Policy clearly defining information security responsibilities of both employees and contractors.
 - Formal assignment of responsibilities of information security to a specific individual(s), position, or team.
 - Formal assignment of responsibilities for creating and distributing security incident response and escalation procedures to a specific individual(s), position, or team.
- Security Awareness:
 - Policy document defining the formal security awareness program that is required for all employees working within the cardholder environment.
- Cardholder Storage & Retention Procedures:
 - Process document detailing how sensitive authentication data that is received is securely deleted and not stored. (track data, CVC, PIN, etc.)
- Rogue Wireless Detection Procedures:
 - Process detailing how to:
 - Detect wireless access points
 - Identify unauthorized wireless access points
 - Perform the process (at least) on a quarterly basis
 - Process detailing how to detect and identify unauthorized wireless access points, including:
 - WLAN cards inserted into system components
 - Portable wireless devices connected to system components

- Wireless devices attached to a network port or network device
- Any other unauthorized wireless access points"
- Process detailed in the Incident response plan on how to respond if unauthorized wireless devices are detected
- Vulnerability Scanning Procedures:
 - Process detailing requirements and steps for performing rescans as part of the quarterly internal scan process until passing results are obtained.
 - Process detailing the Identify of the internal and/or external resources who performed the quarterly scan
 - Process detailing how and when to perform internal and external scans after any significant changes
- System Configuration Standards Documentation must include the following requirements:
 - Configuration Standard documentation specifying each enabled service, daemon and protocol necessary for each system component.

Revision 2.1 Updates

- Security awareness section was updated to document existing requirements for department based regulatory testing and reseller policies
- Physical security section updated to outline physical audit requirement standards



Acknowledgment of Comprehensive Security Policy

This form is used to acknowledge receipt of, and compliance with, the Sarima Comprehensive Security Policy.

Procedure

Complete the following steps:

1. Read the Sarima Comprehensive Security Policy.
2. Sign and date in the spaces provided below.
3. Return the signature pages only to the Human Resources department.

Signature

By signing below, I agree to the following terms:

- I. I have received and read a copy of the "Sarima Security Policy" and understand the same;
- II. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and Confidential Information about Sarima and its customers or its vendors, and that this is and remains the property of the company at all times;
- III. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at Sarima), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
- IV. I understand that Sarima reserves the right to use any method they deem fit to ensure that this policy is followed and that no information on my computer, laptop or other company provided equipment is excluded from possible review in order to verify compliance with this policy;
- V. I agree that, if I leave Sarima for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control;
- VI. I understand that the most current version of this document is located at <http://www.sarimazine.com/resources/secpolicy/> and that I am responsible for reviewing this document for its content and will reaffirm the noted acknowledgement of the policy annually.

Employee signature: _____

Employee name: _____

Date: _____

Department: _____



FEDERAL COMPUTER FRAUD AND ABUSE ACT
TEXAS COMPUTER CRIMES STATUTE
SARMA EMPLOYEE DISCLOSURE AND COMPLIANCE STATEMENT

I hereby certify that my employer, Sarma) has disclosed to me, and I fully understand, the restrictions imposed on me by the Federal Computer Fraud and Abuse Act and the Texas Computer Crimes Statute.

I acknowledge disclosure of and I understand the provisions of the Federal Computer Fraud and Abuse Act, Title 18 U.S.C. 1030, which states:

"Whoever intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) ... shall be punished as provided in subsection "c" of this section."

I understand that violation of the Federal Computer Fraud and Abuse Act may result in a fine and/or term of imprisonment upon conviction.

I further acknowledge disclosure of and I understand the provisions of Section 33 of the Texas Penal Code, entitled "Computer Crimes", which provides that it is a crime to intentionally or knowingly give to an unauthorized person a password, identifying code, personal identification number or other confidential information about a computer security system which restricts the use of a computer or access to data stored or maintained by a computer. Violation of this law may result in fines up to \$2000.00 and/or imprisonment for up to one year.

I am fully aware that this certification is for my protection and that of the company as security measures. Any violation may mean immediate termination of employment as well as possible criminal prosecution for violation of Federal Computer Fraud and Abuse Act and/or the Texas Computer Crimes Statutes.

READ, UNDERSTOOD AND AGREED THIS _____ DAY OF

_____ 20__

EMPLOYEE NAME (PRINT)

EMPLOYEE SIGNATURE



MAEF
Background
ScreeningSM

Employment Screening
System Training

Table of Contents

- Accessing System
 - Sign on
 - Authentication
 - Changing password
 - Requesting password
- Using System
 - Enter Applicant Information
 - Order Services
 - Simple Orders
 - Multi-part Orders
 - County Criminal
 - MVR Report
 - Education
 - Drug Testing
- Transmit Request
- The Status Box
 - Adding Services to Open Profile
 - Printing Reports
 - Special Features
 - Uploading Documents
 - Copying Profile

Accessing the System

- Prior to using our background screening system you will need to first sign up for services. Once approved as a customer of MAF Background Screening you will receive a user code and instructions on using our services.
- Call 800-226-4483 for assistance for additional information or visit us at www.mafscreening.com

Accessing the System

Go to <https://online.mafscreening.com>

Sign on: enter

- Username
- Password
- Click Login

The screenshot shows a login form with the following fields and options:

- Account Login: User Name
- Username:
- Password:
- Remember Username
- Forgot Password?
- Log In

Below the form, there is a message: "Welcome to MSF Background Screening" with a double-headed arrow pointing to the form area.

RETURN TO MENU PAGE

Accessing the System

Authentication

You must Authenticate each PC used

Allow cookies and do not remove browsing history upon exit.

- Answer the Questions
- Click Save

Setup Authentication Questions

An part of our ongoing commitment to help protect you against identity theft and fraud, we help prevent unauthorized access to your accounts while reassuring you that you're at the valid website. Three challenge questions that are secrets between you and us are presented. This helps protect you, whether you're signing into our system from your own computer, or from somewhere else.

Question 1:

Answer 1:

Question 2:

Answer 2:

Question 3:

Answer 3:

*Note: All answers must contain 3 or more characters



[RETURN TO MENU PAGE](#)

Accessing the System

Authentication

- Click Continue to send code to listed e-mail

Authentication Code Delivery Method

Please select the method in which your authentication code will be sent to you. Upon receiving this code you will be able to completely log into the site.

Send to Email: xxxxxxxxxx@mfcreering.com



This code expires in 15 minutes be sure to continue with this process until completed.

If you do not receive your code within a few minutes please call the help desk at 800-226-4483 they will provide the code.

[RETURN TO MENU PAGE](#)

Accessing the System

- Once the authentication code is received highlight and copy the code.
- This is a one time use code, there is no need to retain either the code or the e-mail once authentication is completed.

Note: This is a service message regarding the Authentication Code you requested.

Dear CustomerName,

Here is the Authentication Code you will need to help us recognize your computer.

Your Authentication Code is: 99999999.

This code will expire soon so please enter it in the appropriate field online as soon as possible.

Please follow the instructions below if you are unsure about where to enter your Authentication Code.

- If you are currently on the page where you can enter your Authentication Code, please enter it now.
- If you are *not* currently on our site, then please follow these steps to access your account:
 1. Go to our site as you normally do.
 2. Enter your current password in the Current Password field.
 3. Enter your User ID and Password into the fields on the page and click "Log On."
 4. Answer your random security questions.
 5. On the "Verify Your Identity" page, please click the "I already have a code" button.
 6. Enter the Authentication Code you received in this e-mail in the Authentication Code field.
 7. Click "Continue."

[RETURN TO MENU PAGE](#)

Accessing the System

- Enter (Cut and Paste) Authentication Code

Authentication Code

Your requested authorization code has been sent successfully to your email account.

In order to fully log into this site you must supply the authorization code that was sent to you.

Please enter your authentication code:

Continue

- Click Continue

Each computer used to access the system will have to be authenticated. We know from experience sharing users codes does not work well. We ask each user to have their own codes.

RETURN TO MENU PAGE

Changing Password

You will receive a password from our operations center.

All passwords are one time use and you must change when you first sign on.

Your new password must contain at least:

- 8 characters
- 1 capital letter
- 1 lower case letter
- 1 special symbol (@ # & *)

Please have new password ready before you first sign in.

From: operations@mascreeing.com
To: Your Name
Cc:
Subject: The new password of your account

The password of your user account is reset to: o!%#0ZZ*

You need to change your password at the first time of login.

[RETURN TO MENU PAGE](#)

Changing Password

Enter the Password of the account you wish to change (Paste)

Set Password

Despite what happens in the media, statistics show that most system hackers DO NOT occur because a hacker broke his way in using computer tricks. Instead, most hackers are accomplished using what hackers call "social engineering." Meaning they call a person up on the phone, pretend to be a system administrator or your person, and trick that unsuspecting person into giving out his password. Please, keep in mind that the operators of this site will NEVER call you or email you to ask for your password. Do not tell your password to anyone.

You can use this form to change your password. First, please enter your current password, then enter your new password twice.

Enter Current Password:

.....

Enter New Password:

.....

Confirm New Password:

.....

Click Submit

Your new password must conform to the following rules:

- Must be at least 8 characters (and no more than 28)
- Must have at least one lower case letter (more than one is fine)
- Must have at least one UPPER CASE letter (more than one is fine)
- Must have at least one number (more than one is fine)
- Must have at least one special or punctuation character, such as %, @, !, ", or & (more than one is fine)

These stringent password rules are essential to the security of the system.

Also, please keep the following security guidelines in mind:

- Protecting your password is your responsibility
- Please, choose a password that is easy for you to remember but difficult for someone else to guess
- Please, never share your password with anyone
- Please, do not keep your password written down where someone might find it
- Please, do not give out your password to anyone over the phone
- Please, be sure and change your password immediately if you ever have reason to believe someone else might have learned your password

[RETURN TO MENU PAGE](#)

Changing Password

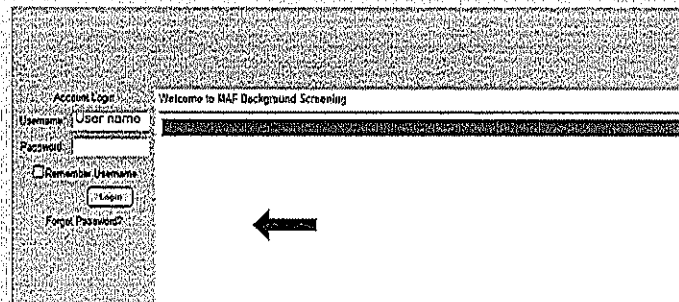
Forgot your password or want a new one?

Go to sign on
page:

Enter:
Username

Click Forgot
Password.

System will send you a new password by E-mail
Follow the normal process to update your password.



The screenshot shows a web page titled "Welcome to MAF Background Screening". On the left side, there is a login form with the following elements: "Account Login", "Username: User name", "Password:", "Remember Username", a "Login" button, and a "Forgot Password" link. A black arrow points to the "Forgot Password" link. The main content area of the page is currently blank.

[RETURN TO MENU PAGE](#)

Using System

New Request

The screenshot shows a sidebar menu with a 'Profiles' section. The 'Profiles' section is expanded, showing a list of options. A callout box points to the 'Create New Profile' option.

- Profiles
 - Create New Profile
 - View All Profiles
 - Draft Profiles
 - In Progress Profiles
 - With Status Detail
 - With Service Alerts
 - In Review
 - With Flagged Orders
 - Completed Profiles
 - With Flagged Orders
 - Archived Profiles
 - Having Document(s)
- Search

Click On
Create New Profile

To enter a new Request

Click on Create New Profile

The "Profile" is the information on
your applicant

RETURN TO MENU PAGE

Using System

New Request

Enter Profile Information

Applicant Information							
First Name:	<input type="text"/>	Middle:	<input type="text"/>	Last Name:	<input type="text"/>	Suffix:	<input type="text"/>
SSN:	<input type="text"/>	Validate U.S. SSN:	<input checked="" type="checkbox"/>	Birth Date:	<input type="text"/>		
Address1:	<input type="text"/>	Address2:	<input type="text"/>	City:	<input type="text"/>	Zip:	<input type="text"/>
Country:	<input type="text"/>		State:	<input type="text"/>	County:	<input type="text"/>	
Email:	<input type="text"/>	Account codes:	<input type="text"/>	Phone No.:	<input type="text"/>	Position:	<input type="text"/>
Acct. Code:	<input type="text"/>	Folder:	<input type="text"/>	Comments:	<input type="text"/>		
				State List:			
				AK			
				AL			
				AR			
				AZ			
				CA			
				CO			
				CT			
				DC			
				DE			
				FL			
				GA			
				GU			
				HI			
				IA			
				ID			
				IL			
				IN			
				KS			

The more common the name the
Include Suffix if applicant is JR, SR, II
Enter SSN with or without the dashes
DOB formats mm/dd/yr; mmdyy
Address2 is for Apt, lot or suite number
Account Code can be used to group
Department

Highlighted:

RETURN TO MENU PAGE

New Request

New Request

Order Services

Simple services can be run using just the information from the profile.
Social Security Number * National Criminal Database * Credit Report

Some services however require additional information
MVR * County Criminal * State Criminal * Education Verification * Employment Verification

Drug testing is a special service linking Drug testing into the system

Electronic Chain of Custody or
Standard paper Chain of Custody including DOT

[RETURN TO MENU PAGE](#)

New Request

New Request

Order Services

Applicant Information		
Name: John Doe	Profile: 2012011757671447	Total Cost:
Address: 123 main, Tampa, FL 33602	Birth Date: 01/01/1961	SSN: 111-22-3344
County: Hillsborough	Country: UNITED STATES	
Email Address:	Phone No.:	
Acct. Code:	Position:	
Entered:	Entered By:	
Status: Draft	Edit Edit w/ Comments (0 Name Mappings) (0 SSN Matches) (0 Profile Documents)	

Profile Settings (Internal Use Only)	
Folder: [All Profiles]	Highlighted:
Comments:	
Internal Notes:	

Other Names: 0

Other Addresses: 0

Services Ordered:
<input checked="" type="checkbox"/> Education Verification
<input checked="" type="checkbox"/> Employment Verification
<input checked="" type="checkbox"/> WebCCF-5 Panel Update
<input checked="" type="checkbox"/> NATIONAL CRIMINAL DATABASE 50 STATE (R)
<input type="checkbox"/> 29926785
<input type="checkbox"/> EDUCATION
<input type="checkbox"/> 28026784

Simple services only need information from the profile. Services when marked with a green ball are ready to transmit.

Available Services To Order
<input type="button" value="Close Profile"/> <input type="button" value="Transmit Request"/> <input type="button" value="Delete Request"/> <input type="button" value="View Streamline Detail"/>
<input type="button" value="View Streamline Details"/>

RETURN TO MENU PAGE

New Request

New Request

Order Services

Applicant Information		
Name: John Doe	Profile: 2012011757671447	Total Cost:
Address: 123 main, Tampa, FL 33602	Birth Date: 01/01/1961	SSN: 111-22-3344
County: Hillsborough	Country: UNITED STATES	
Email:	Phone No.:	
Address:	Position:	
Acct. Code:	Entered By:	
Entered:		
Status: Draft		
Print Print w/ Comments (0 Name matches) (0 SSN matches) (0 Profile Documents)		
Profile Settings (Internal Use Only)		
Folder: [All Profiles]		Highlighted:
Comments:		
Internal Notes:		
Other Name: 0		
Other Address: 0		
Services Ordered		
● Education Verification		
● WebCCF-5 Panel Update		
● NATIONAL CRIMINAL DATABASE 50 STATE (R)		
● 29826785		
● Education Employment Verification SMN pkg		
● 29826784		
Available Services To Order		
Close Profile Transfer Request Delete Request View Streamline Detail View Streamline Detail		

To enter the required information click on the icon with the green plus sign

RETURN TO MENU PAGE

New Request

New Request

County Criminal Search

Items entered are required.

Use Values Entered

COUNTY CRIMINAL: Order Criteria **Required Information**

Names
 John Q. Doe

Addresses
 123 Main, Tampa, FL 33602

Use Values Entered Use Values From Selected Addresses Use Both Values

Alert: Any New York county that has a \$50.00 surcharge is a statewide report. THERE IS NO NEED TO ORDER ANY OTHER NY COUNTIES.

Enter State

Enter/Select County

Enter Gender

City

Zip Code

Locate
Find a City
Find a Zip Code

Enter City or Zip

If you do not know the county use the locator tools
Click to expand/collapse Special Instructions area.

Click save

[RETURN TO MENU PAGE](#)

New Request

New Request

County Criminal Search

Enter your selection

Use Values From Selected Addresses

COUNTY CRIMINAL Order Criteria (Required Information)

Names

John Q. Doe

Addresses

123 Main, Tampa, FL 33602

Use Values Entered Use Values From Selected Addresses Use Both Values

Alert: Any New York county has a \$66.00 surcharge is a statewide report. THERE IS NO NEED TO ORDER ANY OTHER NY COUNTIES.

Click on Address or Addresses you want searched

State =

County =

City =

Zip Code =

Locate

Find a City

Find a Zip Code

Enter Gender

Gender =

Click to expand/collapse Special Instructions area.

Click save

RETURN TO MENU PAGE

New Request

New Request

MVR

Mano a Mano Simón Rodríguez Clujana es un portal de información que ofrece a los usuarios un servicio de atención al cliente en línea.

*** PUERTO RICO NOW REQUIRES COPY OF DRIVERS LICENSE ***

State *

License Number *

Year *

Gender (WF) (Read CA Only)

Use Validate Format to determine reason DL is Invalid

RETURN TO MENU PAGE

New Request

New Request

Education

Education Verification Order Criteria **Required Information**

Names
 John Q. Doe

Addresses
 123 Main, Tampa, FL 33602

School Name:

School City:

School State:

School Phone Number:

Dates Attended:

Degree Claimed:

Click to expand/collapse Special Instructions area.

Click Save and Add Another if you want to enter a second school.

Enter school Name

Enter City where school is located

Enter State where school is located

Although not required these items are extremely important and many checks cannot be done without them

RETURN TO MENU PAGE

New Request

New Request

Drug Testing

Request of list of closest sites to zip. If list is too short, increase distance and try again.

Search Radius: Miles

Person ID: Person Name: Phone Number: Order Information:

Gender: Place Served: State:

Registration Expiration: S: PH: E:

Work Phone: Home Phone:

Email Address:

For multiple email addresses use a semicolon and no space between addresses.
Example: john.d@company.com;jane.smith@company.com

RETURN TO MENU PAGE

New Request

New Request

Drug Testing

Select the lab, either Labcorp or Quest closest to your office or location of the applicant.

Lab Name	Address	Phone
<input type="checkbox"/> LABCORP	3 5810 W LA SALLE CT, TAMPA, FL 33607	(813) 976-5227
<input type="checkbox"/> LABCORP	3 7727 W DK MLK BLVD, TAMPA, FL 33607	(813) 977-7110
<input type="checkbox"/> LABCORP		
<input type="checkbox"/> Quest Diagnostics - Tampa - CR293	Tampa, FL 33626	(813) 926-7923
<input type="checkbox"/> Quest Diagnostics - Tampa - DQ1		
<input type="checkbox"/> Quest Diagnostics - Tampa - H93		
Lab Name	Address	Phone
<input type="checkbox"/> Alpha Laboratory - Tampa	2 1864 W Columbus Dr, Tampa, FL 33607	(727) 276-5506
<input type="checkbox"/> InGenix Medical - Tampa (Preferred)	3 2424 W Swann Ave, Tampa, FL 33609	(813) 276-7073
<input type="checkbox"/> Any Lab Test (29) - Tampa (Preferred)	2 2427 West Kennedy Blvd, Tampa, FL 33609	(813) 609-5225

Out of network labs are charged additional fees for collection.

Drop-downs:
Reason For Test: Please Select
County: Please Select State: FL
Registration Expiration: 3/22/2012
Work Phone: Home Phone:

For multiple email addresses use a semicolon and no space between addresses.
Example: john.doe@labcorp.com; jane.smith@quest.com

RETURN TO MENU PAGE

New Request

New Request

Drug Testing

When entering e-mail addresses use your applicants or hiring manager e-mail address depending on where the form is given to applicant. Always include your e-mail address so you will get a copy as well, separate each e-mail with a semi-colon

<input type="checkbox"/> LABCO	<input type="checkbox"/> LABCO
<input checked="" type="checkbox"/> LABCO	<input type="checkbox"/> LABCO
<input type="checkbox"/> LABCO	<input type="checkbox"/> LABCO

Request #

Request Description

Quest Diagnostics Tampa - FL	11	23513 Sheldon Rd, Tampa	(813) 974-7922
Altra Laboratory - Tampa (Preferred)	2	2860 W. Columbus Dr, Tampa	
LabCorp Medical Group (Preferred)	3	2605 W. Swann Ave, Tampa	
Abu Lab Test Flow - Tampa (Preferred)	3	3927 West Kennedy Blvd	33609

Reason For Test *Please Select

- Pre-Employment
- Random
- Post Accident
- Reasonable Suspicion/For Cause
- Follow-Up
- Fitness for Duty
- Promotion
- Other

Gender

Region

Eastern

655-1111

mail.com

Please list email addresses

mailto:cmo@my.com

Click Save

Save


Cancel

RETURN TO MENU PAGE

New Request

New Request

As orders are completed, each will be marked with a green ball

Profiles Create New Profile View All Profiles Ed Pfeiffer Sun Padre Search Find: In: Profile <input type="checkbox"/> Include Stopped <input type="checkbox"/> Highlighted <input checked="" type="checkbox"/> Exact Reports Customer Reports Admin My Customers My Users My Invoices Customer Service  Sorry User Help	Applicant Information Name: John Q. Doe Profile: 2012021027912830 Total Cost: Address: 223 Main, Tampa, FL 33602 Birth Date: 01/01/1963 SSN: 111-22-3344 - A County: Hillsborough Email: Address: ACCT. Code: Entered: Status: Draft Phone No.: Position: Entered By: Profile Settings (Internal Use Only) Folder: [All Profiles] Highlighted: Comments: Internal Notes: Other Names: 0 Other Addresses: 0 CABON VERIFICATION Motor Vehicle report (MVU) WebCCF S Panel Mail NATIONAL / MULTI-STATE CRIMINAL DATABASE (EMP) 2913367 ANN/NAME MATCH 7183304 Available Services To Order <input type="button" value="Close Profile"/> <input type="button" value="Remove Request"/> <input type="button" value="Delete Request"/> RETURN TO MENU PAGE
---	--

When all orders are complete
Transmit your Request

Processing Reports

Adding Orders to Existing Profile

Orders can ONLY be add, if Profile is in Draft or In Progress Status

Status	Count	Count	Count	Count	Count	Count	Count	Count	Count
Draft	0	4	0	2	0	0	0	0	0
In Progress	0	4	0	2	6	0	0	0	0
Status Detail	0	4	0	2	6	0	0	0	0
Service Alert	0	0	0	0	0	0	0	0	0
In Review	0	0	0	0	0	0	0	0	0
Flagged	0	2	0	2	4	0	0	0	0
Complete	0	0	0	0	6	0	0	0	0
Flagged	0	0	0	0	5	0	0	0	0
Archived	0	0	0	0	27	N/A	0	0	0

Completed Profiles since last logged in
Completed Profiles in the last 24 hours

List of In Progress Profiles, 24 to 48 Hours Old

Print w/ Comments
 Sort By: Last Name
 Desc: Desc
 Profiles per page: |
 Reload | Back | Next
 Detailed View
 Folder:
 Profiles 1 to 4 of 4

Profile #	Name	SSN/ID	Status	Folder
2012040334120607	Taine xxxxxxxxxxxx	xxx-xx-9670	In Progress	
Entered on 04/03/2012 09:51 AM by xxxxxxxxxxxx 3 of 7 Orders have been completed (43%)				
2012040332872743	xxxxxxxxxxxxxxxx	xxxx-8761	In Progress	
Entered on 04/03/2012 04:27 AM by xxxxxxxxxxxx 2 of 4 Orders have been completed (50%)				
2012040335355620	Charles xxxxxxxxxxxx	xxx-xx-6744	In Progress	
Entered on 04/03/2012 09:56 AM by xxxxxxxxxxxx 3 of 5 Orders have been completed (60%)				
2012032067301517	Audrey xxxxxxxxxxxx	7672	In Progress	
Entered on 04/03/2012 05:06 AM by xxxxxxxxxxxx 2 of 7 Orders have been completed (29%)				

Click on Profile Number to Open Profile

RETURN TO MENU PAGE

Processing Reports

Adding Orders to Existing Profile

Services Ordered: STATE CRIMINAL REPOSITORY County: Chaves

31253Z

SEARCHED: INDEXED: SERIALIZED: FILED:

COUNTY: ALL COUNTY FEES MAY APPLY. FEES TO ALSO MUST GIVE PLACE OF BIRTH AND MOTHERS MARYEN (MAY)

Education Verification:

Employment Verification:

MOTHER/EDUCATIONAL REQUESTS CALL FOR PRICING

MOTHER/VEHICLE REPORT:

NATIONAL / MULTI-STATE CRIMINAL DATABASE (S):

Notes: This is a 15min & Drop of firm report. NOT ALL ORIGINAL JURISDICTIONS ARE COVERED IN EACH STATE. INCLUDES DMV, SOCIAL OFFENDERS & WHEN CONV. SENTENCES LIST. PLEASE CHECK THE "CRIMINAL DATA SOURCES" FOUND ON THE "REFERENCES PAGE" FOR COMPLETE DESCRIPTIONS OF STATE SOURCES.

SSN/NAME MATCH:

YU EMPLOYMENT REPORT:

RETURN TO MENU PAGE

Processing Reports

Adding Orders to Existing Profile

Multiple Entries (Internal Use Only)

Profile: [All Profiles]

Comments:

Internal Orders:

Order # 31892823

Order Description: NATIONAL SEX OFFENDER PUBLIC WEBSITE 30 STATE (N00PW)

Education Verification: NATIONAL CRIMINAL DATA

Join Date: 3/18/2003

FL

Michael Lee

Close Profile

Transmit Enquest

Order Request

View Breakdown Details

Since Profile is in progress, the added service are immediately processed and are not required to be transmitted.

RETURN TO MENU PAGE

Printing Reports

Reports can be printed from two locations in the system

Status	2A	2A-10	4B-12	5-12	Total	Highlights	Notifications
Draft					1	0	0 Completed Profiles since last logged in
In Progress	1	3	0	2	6	0	1 Completed Profiles in the last 24 hours
Status Detail	1	2	0	0	3	0	0 New Profiles since last logged in
Service Alert	1	3	0	2	6	0	1 New Profiles in the last 24 hours
In Review	0	0	0	0	0	0	
Flagged	0	0	0	0	0	0	
Complete					5	0	
Flagged*					1	0	
Archived					10	N/A	

List of Completed Profiles

Print w/ Comments
 Detailed View
 Sort By: Last Name
 Desc Throt: [Select Column]
 Desc
 Profiles per page: 25
 Reload
 Back
 Next
 Profiles 1 to 6 of 6

Profile #	Name	Folder	Completed
2012030730067893	CSMC-D Entered on 03/07/2012 08:27 AM by Ann Completed on 03/12/2012 10:41 AM by CS_SynchProfStatus 5 of 5 Orders have been completed (100%)		COMPLETED
2012030530461517	Loia Entered on 03/05/2012 08:30 AM by Ann Completed on 03/12/2012 10:46 AM by CS_SynchProfStatus 6 of 6 Orders have been completed (100%)		COMPLETED
2012030131328293	Gerald Entered on 03/01/2012 08:44 AM by Ann Completed on 03/09/2012 04:36 PM by CS_SynchProfStatus 10 of 10 Orders have been completed (100%)		COMPLETED
2012030730900697	Ashley Entered on 03/07/2012 08:35 AM by Ann Completed on 03/14/2012 01:48 PM by CS_SynchProfStatus 5 of 5 Orders have been completed (100%)		COMPLETED
2012031241686020	Martin K. Entered on 03/12/2012 11:35 AM by Ann Completed on 03/15/2012 01:54 PM by CS_SynchProfStatus 6 of 6 Orders have been completed (100%)		COMPLETED
2012030532298933	Cynthia Entered on 03/05/2012 09:00 AM by Ann Completed on 03/14/2012 01:45 PM by CS_SynchProfStatus 9 of 9 Orders have been completed (100%)		COMPLETED

Printing Reports

Report opens as a PDF file, print or save as needed.

MAF Background Screening
134 South Tampa Street
Tampa, FL 33602
Phone: (800) 225-4483
Fax: (800) 225-7785
online.mafscreening.com



Requested by:
MAF Test Customer
134 South Tampa Street
Tampa 05618
Phone: 813-273-7010
Fax: 813-277-3651

Applicant Information

Name: John Q Doe	Address: 123 Main
SSN: ***-**-3344	Tampa, FL 33602
DOB: **/**/1961	
Position:	
Acctg Code:	
Status: OPEN	

Special Features

- Uploading Documents
 - Attach release form to profile, make available to others in your office or with MAF as needed by accessing the profile.
 - Release form can be sent to employers or others when need to provide a release, no need to fax copy.
 - Release form is attached to profile and stored on line. If later audited, the profile contains the needed release form showing consent.

Uploading Documents

From the Profile

Employee Information	
Name: John Q. Doe	Profile: 2012761007912310 Total Cost: \$1.00
Address: 132 Maple, Tampa, FL 33602	Birth Date: 01/23/2061 SSN: 11-00-0344
County: Hillsborough	Gender:
Unit Address:	Phone No.:
Accr. Code:	Position:
Entered: 02/10/2013 07:45 AM EST	Entered By: scott@hr
Status: Draft	Profile: 2012761007912310
Profile Summary (Internal Use Only)	
Comments:	Highlighted:
Folder: All Profiles	
Internal Notes:	

Click on "Profile Documents"

Uploading Documents

From the Profile

Name: John Q. Doe Address: 123 Main, Tampa, FL 33602 Profile: 202021027912340 Birth Date: 01/01/1961 SSN: 111-22-3344 Acct. Code:
Entered: 02/10/2012 07:45 AM EST Entered By: epplefer

Status: Draft

Upload New Documents

Document Name Description Date Added Added By Activities

Click on "Upload New Documents"

Uploading Documents

Name: John Q. Doe
Address: 123 Main, Tallahassee, FL 32302
Entered: 02/10/2012 07:40 AM EST
Status: Open

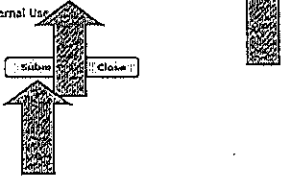
Profile: 201201027011020
Birth Date: 01/01/1991
Entered By: administrator
SSN: 111-22-3344
Acct. Code:

Upload New Document

Document To Upload:

Description:

Internal Use



Select the document you want from your hard drive to load to the system




Name document for your identification

Click Submit

Uploading Documents

Applicant Information			
Name: John Q. Doe	Profile: 2012021027912530	Birth Date: 01/01/1991	SSN: 111-22-3344
Address: 123 Main, Tampa, FL 33602	Entered By: edp/feffer	Accr. Code:	
Entered: 02/10/2012 07:45 AM EST	Status: Draft		

Upload New Document

Document Name	Attached Document Description	Date Added	Added By	Actions
GENERAL RELEASE Cheat form.pdf	Name of Document	7/22/2012	edp/feffer	  

To delete a file click on "trash can"

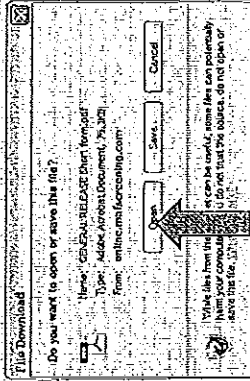
To update current document click on green arrow

To open file, click on red arrow

Uploading Documents

Applicant Information			
Name: John Q. Doe	Profile: 20120102791200		
Address: 123 Main, Tenn., TN 31602	Birth Date: 01/01/1951		
Entered: 02/01/2012 07:45 AM EST	SSN: 11-35-3344		
Entered By: espilifer	Acct. Code:		
Attached Documents			
Document Name	Description	Date Added	Added By
GENERAL RELEASE Short Term.pdf		7/25/12	espilifer

Click on "open"



Special Features

Copying Profiles

You may copy information from one profile into a new profile quickly and easily.

Special Features

Copying Profiles

Client Profiles

Client Profiles

1. Select Profiles to Copy

2. Copy Profiles to Client Profile

3. Copy Profiles to Client Profile

4. Copy Profiles to Client Profile

5. Copy Profiles to Client Profile

6. Copy Profiles to Client Profile

7. Copy Profiles to Client Profile

8. Copy Profiles to Client Profile

9. Copy Profiles to Client Profile

10. Copy Profiles to Client Profile

Profile Name	Profile ID	Profile Type	Profile Status
Example Profile	0000000001	Example	Completed
Example Profile	0000000002	Example	Completed
Example Profile	0000000003	Example	Completed
Example Profile	0000000004	Example	Completed
Example Profile	0000000005	Example	Completed
Example Profile	0000000006	Example	Completed
Example Profile	0000000007	Example	Completed
Example Profile	0000000008	Example	Completed
Example Profile	0000000009	Example	Completed
Example Profile	0000000010	Example	Completed

List of Completed Profiles

1. Select Profiles to Copy

2. Copy Profiles to Client Profile

3. Copy Profiles to Client Profile

4. Copy Profiles to Client Profile

5. Copy Profiles to Client Profile

6. Copy Profiles to Client Profile

7. Copy Profiles to Client Profile

8. Copy Profiles to Client Profile

9. Copy Profiles to Client Profile

10. Copy Profiles to Client Profile

Profile Name	Profile ID	Profile Type	Profile Status
Example Profile	0000000001	Example	Completed
Example Profile	0000000002	Example	Completed
Example Profile	0000000003	Example	Completed
Example Profile	0000000004	Example	Completed
Example Profile	0000000005	Example	Completed
Example Profile	0000000006	Example	Completed
Example Profile	0000000007	Example	Completed
Example Profile	0000000008	Example	Completed
Example Profile	0000000009	Example	Completed
Example Profile	0000000010	Example	Completed

Special Features

Copying Profiles

Select one,

No services, only copy the applicant information

Add only pre-selected services

Add all services for the old profile

A copy of the selected profile(s) is about to be created.
Please select how the services are added to the new profile.
If you select to add services, orders will ONLY be created for the SIMPLE services.

- No services, only copy the applicant information.
- Add only pre-selected services.
- Add all services from the old profile.

Create Copy

Click Create Copy

Draft is created and can be opened in the status box to complete the ordering process.

For Assistance

Contact our help desk for assistance or questions.

800-226-4483 - operations@mascreeing.com