MARIPOSA COUNTY

HHS/Social Services · (209) 966-2000

RESOLUTION - ACTION REQUESTED 2021-520

MEETING: September 15, 2021

TO: The Board of Supervisors

FROM: Shannon Gadd, Health and Human Services Agency Director

RE: Approve Agreement with Binti, Inc.

RECOMMENDATION AND JUSTIFICATION:
Approve an Annual Subscription Agreement with Bitini, Inc. to Provide Software Services for Foster Care Case Management; and Authorize the Health and Human Services Agency Director to Sign the Agreement.

Founded in 2017, Binti, Inc. (Binti) has partnerships with county and state government entities as well as private agencies across 24 states to improve foster care. For this agreement, Binti will implement its Software-as-a Service platform to allow for Mariposa County Health and Human Services Agency (HHSA) staff to track and manage ongoing paperwork and requirements for children and youth in our foster care system.

For access to Approvals Platform and Placements Platform and ongoing support and maintenance, HHSA will be assessed an $11,000 fee for each 12-month period. Fees are subject to an increase in an amount not to exceed 3% more than fees during the immediately preceding 12-month period. Beyond the initial three year term, this agreement will automatically renew for additional consecutive terms of 12 months.

BACKGROUND AND HISTORY OF BOARD ACTIONS:
Board of Supervisors does not have a prior history with Binti, Inc.

ALTERNATIVES AND CONSEQUENCES OF NEGATIVE ACTION:
The Board can choose to not authorize this agreement and forego an opportunity for HHSA to ensure effective case management for foster children throughout the County.

FINANCIAL IMPACT:
There is no impact to the General Fund.

ATTACHMENTS:
Binti Master Agreement_Mariposa Country_8_18_2021 (PDF)
Binti Security Plan [04.13.2021] (PDF)

REF ID# 12102

RESULT: **ADOPTED [UNANIMOUS]**
MOVER: Rosemarie Smallcombe, District I Supervisor
SECONDER: Tom Sweeney, District II Supervisors
AYES: Smallcombe, Sweeney, Long, Forsythe, Menetrey

MASTER SUBSCRIPTION AND SERVICES AGREEMENT

This Master Subscription and Services Agreement ("**Agreement**") is made as of **Sept. 15,** 2021 ("**Effective Date**"), between Binti, Inc. with an address at 1212 Broadway, Suite 200, Oakland, California 94612 ("**Binti**"), and Mariposa County with an address at 5362 Lemee Lane, Mariposa, CA 95338 ("**Licensee**"). Binti and Licensee will be referenced to individually herein as "**Party**" and collectively as the "**Parties**."

Binti has developed a Software-as-a-Service platform, as described at www.binti.com ("**Platform**"). The Approvals Platform allows users to apply online to become approved to foster children and allows social workers to manage their approval workflow online. The Placements Platform allows for the matching of child referrals to approved foster families. The Case Management Platform allows agencies to track and manage ongoing paperwork and requirements for children and youth in their care ("**Authorized Purpose**"). This Agreement governs a relationship whereby Binti will (i) grant Licensee access to the Platform; and (ii) perform the professional services set forth in **Exhibit A** attached hereto ("**Professional Services**," together with the Platform, the "**Services**"). Accordingly, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Proprietary Rights.

(a) Platform. Subject to the terms and conditions of this Agreement, Binti hereby grants to Licensee during the Term (defined below) a non-exclusive, non-transferable and non-sublicensable license to allow its employees and contractors who have been issued valid access credentials from Binti ("**Authorized Users**") to access and use the Platform solely to help facilitate foster care and adoptions for children. Binti will provide access to the Service to Authorized Users subject to Binti's Terms of Service, and in its capacity as a data controller, will process the Authorized Users' personal information in compliance with Binti's Privacy Policy. Binti will provide Licensee with the support services set forth in **Exhibit B** attached hereto.

(b) Restrictions. Licensee will not, and will not permit any third party to: (i) copy, modify, translate, or create derivative works of the Platform; (ii) reverse engineer, decompile, disassemble or otherwise attempt to reconstruct, identify or discover any source code, underlying ideas, underlying user interface techniques, or algorithms of the Platform (except to the extent such prohibition is contrary to applicable law); (iii) lend, lease, offer for sale, sell or otherwise use the Platform for the benefit of any third party except as permitted under Section 1(a); (iv) attempt to disrupt the integrity or performance of the Platform; (v) attempt to gain unauthorized access to the Platform or its related systems or networks; or (vi) use the Platform in a manner that violates this Agreement, any third party rights or any applicable laws, rules or regulations.

(c) Binti Ownership. Except for the rights granted to Licensee in Section 1(a) above and Licensee's rights to Data (defined below), as between the Parties, Binti retains all right, title and interest, including all intellectual property rights, in and to the Platform (including all Updates thereto) and all aggregated and de-identified information that Binti's systems or applications automatically collect regarding the Platform and/or its use and/or performance (including, without limitation, de-identified Data that does not, and cannot reasonably be used to, identify Licensee or any individual) ("**Diagnostic Data**") (which, notwithstanding anything to the contrary, Binti may fully exploit). All rights that Binti does not expressly grant to Licensee in this Section 1 are reserved and Binti does not grant any implied licenses under this Section 1.

(d) Licensee Ownership. As between the Parties, Licensee owns all data, information and other materials submitted to the Platform or Binti by Licensee or Authorized Users (which, for clarity, excludes Diagnostic Data) (collectively, "**Data**"). Licensee represents and warrants that: (i) it either owns the Data or is otherwise permitted to grant the license set forth in this Section; (ii) the posting and use of Data on or through the Platform does not violate the privacy rights, publicity rights, copyrights, contract rights, intellectual property rights, or any other rights of any person; and (iii) the posting of Data on the Platform does not result in a breach of contract between Licensee and any third party. Licensee hereby grants to Binti a non-exclusive and non-transferable (except under Section 10) license to use and host the Data, solely to provide the Services. Binti is not responsible for the content of any Data or the way Licensee or its Authorized Users choose to use the Platform to store or process any Data. Upon termination or expiration of this Agreement for any reason, Binti will permit Licensee to download all Data from the Platform in .csv format.

2. Use of the Services.

(a) Binti's Obligations. Binti will use commercially reasonable efforts to make the Service available at all times, except for planned downtime and any unavailability caused by Force Majeure Events (defined below). Binti will maintain commercially reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Data.

(b) Licensee's Obligations. Licensee acknowledges and agrees that it is responsible for the use or misuse of the Service by Authorized Users, and a breach by any Authorized User of any term of this Agreement will be deemed a breach by Licensee of this Agreement. Licensee acknowledges and agrees that the Licensee and Licensee's Authorized Users use

of the Platform is in compliance with all applicable laws, and Licensee acknowledges that Licensee assumes all risk arising from any such use that is not compliant with applicable laws.

3. Professional Services.

(a) General. Subject to Licensee's compliance with the terms and conditions of this Agreement, Binti will perform the Professional Services in accordance with any specifications set forth in **Exhibit A**. Each Party will communicate with the point of contact set forth in **Exhibit A** in connection with the Professional Services. Licensee will reasonably cooperate with Binti to facilitate provision of Professional Services. This cooperation will include, without limitation, (i) performing any tasks reasonably necessary for Binti to provide the Professional Services and to avoid unnecessary delays; (ii) fulfilling any Licensee obligations described in **Exhibit A** in a timely manner; and (iii) responding to Binti's reasonable requests related to Professional Services in a timely manner. Notwithstanding anything in **Exhibit A** to the contrary, Binti will not be liable for any delays in performing the Professional Services that arise, in whole or in part, from Licensee's acts or omissions, including, without limitation, its failure to comply with this Section 3(a).

(b) Intellectual Property Rights. Binti solely owns all right, title and interest in and to any software, notes, records, drawings, designs or other copyrightable materials, inventions (whether or not patentable), improvements, developments, discoveries and trade secrets conceived, discovered, authored, invented, developed or reduced to practice by Binti, solely or in collaboration with others, arising out of, or in connection with, Binti performing the Professional Services, including any copyrights, patents, trade secrets, mask work rights or other intellectual property rights relating to the foregoing ("**Inventions**"). Binti hereby grants to Licensee a non-exclusive, non-transferable, non-sublicensable, royalty-free and worldwide right during the Term to use the portion of the Inventions that is incorporated into any deliverables that Binti provides to Licensee under **Exhibit A** solely to use any such deliverables. Binti reserves all rights not expressly granted in the prior sentence and does not grant any implied licensed under this Section 3.

4. Fees.

(a) Fees. Licensee will pay Binti [(i) $11,000 for access to the Approvals Platform and Placements Platform for each 12-month period and for Professional Services set forth in Sections 2(a)-(b) of Exhibit A hereto (collectively, "**Fees**"). All Fees will be due and payable within thirty (30) days from the date of the applicable invoice issued by Binti. Except as expressly set forth herein, all Fees are non-cancellable and non-refundable. Late Fee payments will accrue interest at the rate of one-and-one-half percent (1.5%) of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, from the date such payment was due until the date paid.

(b) Fee Increases. Binti in its sole discretion may increase the fees due for any 12 month period during the Term in an amount not to exceed 3% more than the fees payable during the immediately preceding term of the same length to adjust for inflation; provided, however, that Binti may increase the fees by an amount deemed necessary by Binti in its sole discretion during any Renewal Term in connection with enhancements and/or improvements made to the Platform or Professional Services.

(c) Taxes. The Fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any applicable taxing authorities (collectively, "**Taxes**"). Licensee is responsible for paying all Taxes associated with its receipt of the Services (except for any Taxes based on Binti's net income).

5. Confidential Information.

(a) Definition of Confidential Information. As used herein, "**Confidential Information**" means all confidential information disclosed by a Party ("**Disclosing Party**") to the other Party ("**Receiving Party**"), that is marked in writing as "confidential" or by a similar designation. For clarity, Confidential Information of Binti also includes the Binti technology underlying the Platform and any related non-public specifications, documentation or technical information that Binti makes available to Licensee. Confidential Information will not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party without restriction prior to its disclosure by the Disclosing Party and without breach of any obligation owed to the Disclosing Party; (iii) is received from a third party without restriction and without breach of any obligation owed to the Disclosing Party; or (iv) was independently developed by the Receiving Party without use of or reference to any Confidential Information of the Disclosing Party.

(b) Protection of Confidential Information. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care). The Receiving Party may only use Confidential Information of the Disclosing Party to perform its obligations or exercise its rights under this Agreement. Except as expressly authorized by the Disclosing Party in writing, the Receiving Party will limit access to Confidential Information of the Disclosing Party to those of its and its affiliates' employees, contractors or

agents who need such access to perform obligations under this Agreement and who agree to abide by the terms set forth in this Section 5.

(c) Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

6. Term and Termination.

(a) Term. This Agreement will commence on the Effective Date and continue for a period of thirty-six (36) months ("**Initial Term**"). Thereafter, this Agreement will automatically renew for additional consecutive terms of twelve (12) months (each, a "**Renewal Term**," together with the Initial Term, the "**Term**"), unless either Party provides to the other a written notice, at least thirty (30) days prior to the expiration of the then-current Renewal Term, of its intention not to renew this Agreement.

(b) Termination. Either Party may terminate this Agreement for any or no reason (in its sole and absolute discretion), upon written notice to the other Party. Either Party may terminate this Agreement upon thirty (30) days' prior written notice if the other Party is in material breach of this Agreement and the breaching Party fails to remedy such material breach within the thirty (30)-day notice period. Upon termination (except for termination by Binti pursuant to the immediately preceding sentence), the Licensee will have access to the Platform for the remainder of the then-current Term. Upon termination by either party for any reason, Binti will supply the Licensee with an export of the Licensee's Data.

(c) Effect of Termination. Upon expiration or termination of this Agreement for any reason, the licenses granted by each Party will automatically terminate and all outstanding Fees owed pursuant to Section 4 will become immediately due and payable. The provisions of Sections 1(b), 1(c), 2(b), 3(b), 4, 5, 6(c), 7, 8, 9, 10 and all defined terms used in those Sections will survive any expiration or termination of this Agreement.

7. Representations and Warranties.

(a) Mutual. Each Party represents and warrants that: (i) it has the right, power and authority to enter into this Agreement and to grant the rights and licenses granted hereunder and to perform all of its obligations hereunder; (ii) the execution of this Agreement by its representative whose signature is set forth at the end hereof has been duly authorized by all necessary organizational action of the Party; and (iii) when executed and delivered by both Parties, this Agreement will constitute the legal, valid and binding obligation of such Party, enforceable against such Party in accordance with its terms.

(b) Licensee. Licensee further represents and warrants that: (i) it owns or otherwise has sufficient rights to the Data to grant the license set forth in Section 1(d); and (ii) no Data submitted to the Platform does or will violate the privacy, intellectual property or other rights of any person or entity or any applicable laws, rules or regulations.

(c) EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES SET FORTH UNDER THIS SECTION 7, THE SERVICES AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT BY BINTI ARE PROVIDED ON AN "AS-IS" BASIS, AND LICENSEE ASSUMES ALL RESPONSIBILITIES FOR SELECTION OF THE SERVICES TO ACHIEVE LICENSEE'S INTENDED RESULTS, FOR THE ACCURACY AND/OR QUALITY OF ITS DATA, AND FOR ITS USE OF, AND RESULTS OBTAINED FROM, THE SERVICES. BINTI DOES NOT WARRANT THAT THE SERVICES OR ANYTHING ELSE PROVIDED IN CONNECTION WITH THIS AGREEMENT WILL BE ERROR-FREE OR THAT THE SERVICES WILL WORK WITHOUT INTERRUPTIONS. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 7, BINTI MAKES NO PROMISES, REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE SERVICES, AND BINTI HEREBY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY LOCAL JURISDICTIONAL ANALOGUES TO THE FOREGOING.

8. Limitations on Liability. TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW, (I) EXCEPT WITH RESPECT TO SECTION 9, IN NO EVENT WILL EITHER PARTY'S TOTAL LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE FEES PAYABLE TO BINTI DURING THE TERM; AND (II) EXCEPT TO THE EXTENT SUCH DAMAGES ARE PAID OR PAYABLE TO UNAFFILIATED THIRD PARTIES PURSUANT TO EITHER PARTY'S OBLIGATIONS PURSUANT TO SECTION 9, IN NO EVENT WILL EITHER PARTY HAVE ANY LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, FOR LOST PROFITS, DATA OR OTHER BUSINESS OPPORTUNITIES), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR

OTHERWISE. THIS SECTION 8 DOES NOT LIMIT EITHER PARTY'S LIABILITY FOR INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

9. Indemnification.

(a) Licensee. If a third party asserts a claim (each, a "**Third Party Claim**") against Binti or any of its affiliates, officers, employees or contractors (each, a "**Binti Released Party**") alleging or arising from (a) that any Data infringes, violates, or misappropriates any intellectual property or proprietary right(s), (b) that any Data, or its provision to Binti, violates any applicable law or regulation, or (c) any negligent act or intentional misconduct by Licensee or any of its Authorized Users in connection with the Service, then Licensee will defend the Binti Released Party from the Third Party Claim and hold such Binti Released Party harmless from and against all damages, settlements, costs, and/or expenses, in each case, that are paid or payable to third party(ies) with respect to the Third Party Claim (including, without limitation, reasonable attorneys' fees).

(b) Binti. If a Third Party Claim is asserted against Licensee or any of its affiliates, officers, employees or contractors (each, a "**Licensee Released Party**") alleging that the Platform (not including any Data) infringes, violates, or misappropriates such third party's intellectual property or proprietary right(s) ("**Infringement Claim**"), then Binti will defend the Licensee Released Party from the Infringement Claim and hold such Party harmless from and against all damages, settlements, costs, and/or expenses, in each case, that are paid or payable with respect to the Infringement Claim (including, without limitation, reasonable attorneys' fees). In the event of an Infringement Claim, Binti, at its sole option and expense, may: (i) procure for Licensee the right to continue using the Platform or infringing part thereof; (ii) modify the Platform or infringing part thereof; (iii) replace the Platform or infringing part thereof with other software having substantially the same or better capabilities; or, (iv) if the foregoing are not commercially practicable, terminate this Agreement and repay to Licensee a pro-rata portion of the Fees. Notwithstanding the forgoing sentences of this Section 9(b), Binti will have no liability for an Infringement Claim if the actual or alleged infringement results from (a) any breach of this Agreement by Licensee or any Authorized Users; (b) any modification, alteration or addition made to the Platform by Licensee or any Authorized Users, including any combination of the Platform with software not provided by Binti; (c) any failure by Licensee or any Authorized Users to use any Updates made available by Binti; or (d) any settlements entered into by Licensee or costs incurred by Licensee for the Infringement Claim that are not pre-approved by Binti in writing.

(c) Procedures. Each Party's obligations pursuant to Sections 9(a) and 9(b) above (respectively) are expressly conditioned on: (a) the Party seeking indemnification under this Section 9 ("**Indemnified Party**") providing the other Party ("**Indemnifying Party**") with prompt written notice of the applicable Third Party Claim for which the Indemnified Party seeks indemnification; (b) the Indemnified Party reasonably cooperating in the defense and/or settlement of such Third Party Claim, at the Indemnifying Party's sole expense; and (c) the Indemnifying Party having sole control over the defense and/or settlement of such Third Party Claim. The Indemnifying Party may not agree to any settlement of any Third Party Claim against the Indemnified Party that admits wrongdoing by the Indemnified Party, or otherwise imposes any material obligation on the Indemnifying Party (not entirely covered by an indemnification obligation hereunder), without the Indemnified Party's prior express written consent, which consent will not be unreasonably withheld, conditioned or delayed. The Indemnified Party may participate in the defense of a Third Party Claim through counsel of its own choice at its own expense.

10. Miscellaneous. Each Party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other Party, entitling such Party to seek injunctive relief in addition to all available remedies. Neither Party may assign this Agreement or any rights under it, in whole or in part, without the other Party's prior written consent; provided that either Party may assign this Agreement or any rights under it without prior written consent to a successor in connection with a merger, acquisition, reorganization, consolidation, or sale of all or substantially all of its assets or the business to which this Agreement relates. Any attempt to assign this Agreement other than as permitted above will be void. If any provision of this Agreement is held by a court of competent jurisdiction to be unenforceable, then the remaining provisions of this Agreement will remain in full force and effect. This Agreement will be governed by and construed under the laws of California without reference to its conflict of laws principles. This Agreement, including all Exhibits attached hereto, embodies the entire agreement between the Parties with respect to the subject matter set forth herein and supersedes any previous or contemporaneous communications, whether oral or written, express or implied. This Agreement may be modified or amended only by a writing signed by both Parties. If there is any conflict or inconsistency between the terms of any Exhibit and the terms in the body of this Agreement, then the terms in the body of the Agreement will control solely to the extent of the conflict. All waivers made under this Agreement must be made in writing by the Party making the waiver. Any notice required or permitted to be given under this Agreement will be effective if it is (i) in writing and sent by certified or registered mail, or insured courier, return receipt requested, to the appropriate Party at the address set forth above and with the appropriate postage affixed; or (ii) sent via email to the following: in the case of Binti: Felicia@binti.com; and in the case of Licensee: jsims@mariposacounty.org. Either Party may change its address for receipt of notice by notice to the other Party in accordance with this Section. Notices are deemed given two (2) business days following the date of mailing, one (1) business day following delivery to a courier,

and/or on the same day a facsimile or electronic mail is sent to the recipient. Binti will not be liable or responsible to Licensee, nor be deemed to have breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement when and to the extent such failure or delay is caused by or results from acts or circumstances beyond the reasonable control of Binti including, without limitation, acts of God, natural disaster, denial or services attacks and/or service provider system outages (collectively, "**Force Majeure Events**"). This Agreement may be signed in counterparts, each of which will be deemed an original, and all of which together will constitute a single agreement.

BINTI, INC.

5AA959D4079

By: Jamie Gray ZorroSign

Name: Jamie Gray

Title: Assistant Secretary

LICENSEE

5AA959D406F

By: Shannon Gadd ZorroSign

Name: Shannon Gadd

Title: Director, Health and Human Services Agency

5AA959D4065

By: Steven W. Dahlem ZorroSign

Steven W. Dahlem, County Counsel

EXHIBIT A

PROFESSIONAL SERVICES

All capitalized terms that are used but not defined in this Exhibit will have the meanings ascribed to them in the body of the Agreement above.

1. Contact. The principal contacts in connection with the Professional Services are as follows:

Binti:	**Licensee:**
Name: Felicia Curcuru	**Name: Julianne Sims**
Title: CEO	**Title: Division Director, Human Services**
Address: 1212 Broadway, Suite 200, Oakland, California 94612	**Address: 5362 Lemee Lane, Mariposa, CA 95338**
Phone: 844-424-6844	**Phone: (209) 742-0889**
Email: partnerships@binti.com	**Email: jsims@mariposacounty.org**

2. Services. Binti will use commercially reasonable efforts to provide the following Professional Services:

(a) Data Migration. Migrate Data into the Platform based on reasonably written instructions from Licensee within 12 weeks of receiving data with documentation from Licensee.

(b) Form Customizations. Customize up to 60 documents provided to Binti by Licensee for inclusion within the Platform within 12 weeks of Licensee providing the documents.

Any additional Professional Services to be performed by Binti will be mutually agreed upon by the Parties in writing and attached to this **Exhibit A** as successively numbered Schedule "A"s (*e.g.*, Schedule A-1, Schedule A-2, etc.).

This **Exhibit A** is accepted and agreed upon as of the Effective Date set forth in the body of the Agreement.

BINTI, INC.

By: Jamie Gray ZorroSign

Name: **Jamie Gray**

Title: **Assistant Secretary**

LICENSEE

By: Shannon Gadd ZorroSign

Name: **Shannon Gadd**

Title: **Director, Health and Human Services Agency**

By: Steven W. Dahlem ZorroSign

Steven W. Dahlem, County Counsel

EXHIBIT B

SUPPORT

All capitalized terms that are used but not defined in this Exhibit will have the meanings ascribed to them in the body of the Agreement above.

1. Support. Binti will provide technical support to Licensee from 6AM-5PM Pacific Standard time Monday through Friday during the Term except for national holidays in the United States and June 19th. Support may be non-live and/or limited for up to four (4) days per year due to staff training. ("**Support**"). To request Support, Licensee must contact Binti via Live Chat within family.binti.com, via phone at 844-424-6844, or via email at help@binti.com. Support will return/answer all messages received outside of the aforementioned hours during the following business day.

(a) Provision of Support. Binti will provide Support to the following Licensee contact: **jsims@mariposacounty.org**. Binti will not be responsible for addressing or resolving Events (defined below) that Binti reasonably determines are caused by Licensee's systems or any misuse of the Platform.

(b) Events. "**Events**" are occurrences that impact the availability of the Platform, except for scheduled downtime, as determined by Binti in its reasonable discretion. Binti distinguishes among four classes of Events as follows:

(i) **Critical Event**: A complete loss of the Platform's functionality such that no user can use the Platform.
(ii) **High Event**: The Platform's functionality is materially impaired such that at least approximately 10% of users cannot use the Platform for its intended purpose. Users have major impact and minimal functionality is available.
(iii) **Medium Event**: An event not meeting the criteria of Critical or High, has a workaround available, which does not negatively impact the User from using the Platform for its intended purpose. Such errors will be consistent and reproducible. Users would lose some level of functionality but are still able to utilize the system.
(iv) **Low Event**: Any other problems or issues, without limitation, any general questions about the Platform or problems that do not rise to Critical, High, or Medium events. Most users would not notice or be impacted if not addressed.

(c) Target Resolution Times. Binti will use commercially reasonable efforts to meet the following target time frames for resolution of Events from the time Binti receives a Support request:

Event Level		**Target Resolution Time**
Critical		**4 hours or better**
High		**24 hours or better**
Medium **Low**		**Binti will provide a response time of 3 business days; resolution will be determined based on an agreed action/remediation plan between the Parties in writing**

(d) Scheduled Maintenance Downtime. Binti will schedule maintenance between the hours of 10PM and 4AM Pacific Standard time. Binti will provide Licensee with reasonable advance written notice of scheduled downtime. Binti may access the Platform during the scheduled maintenance downtimes for maintenance purposes and to implement Updates, bug fixes and/or any other changes that Binti deems necessary or advisable. Outside of scheduled maintenance downtime, Binti maintains a 99.95% system uptime.

(e) Resolution. If Binti has not resolved an Event within the targeted time frame, then, upon Licensee's written request, Binti and Licensee will discuss a resolution plan. From that point forward until the issue is resolved, Binti will notify Licensee's designated contact of the status of resolution at least once daily.

2. Training. The Parties may agree in writing upon commercially reasonable training that Binti will provide to Licensee Authorized Users during the Term. This may include, by way of example only, a web-based tutorial about how to use the Platform. Training will not exceed a total of 25 hours during the Term.

Binti's Security Plan

Binti Overview

Binti builds modern, mobile-friendly software driving measurable results and promoting quality practice in Child Welfare to ensure that every child has a fair chance at life. Binti's Software-as-a-Service (SaaS) platform includes multiple modules that comprise a solution for child welfare agencies to meet Comprehensive Child Welfare Information System (CCWIS) requirements.

As a cloud-based SaaS solution, Binti simply requires a modern web browser to be utilized, without relying on specific hardware and software technology requirements for agencies. Binti is efficient, intuitive, user-friendly, accessible, mobile, and reliable. Our software is engineered to prioritize security, compliance, quality, usability, efficiency, interoperability, and reporting.

Binti's software is written primarily in Ruby-on-Rails and React, backed with a Postgres database. The back-end infrastructure has been developed to accommodate multiple, flexible workflows - for example, Binti's software is used by private, county, and state agencies, many of whom outsource various services to sub-agencies that have their own access and capabilities within Binti. Binti's Engineering and Product Management team, including data and security specialists with decades of experience, are responsible for IT operations and critical business functions. Each Product Manager is responsible for the scope and prioritization of tasks that are carried out by the Engineering team with regards to each module.

Binti Security Practices and Protocol

At Binti, security was integrated into our company from the very beginning and remains a primary focus today. Security is integrated throughout the environment, from the people, to the processes, to the technology. Because we're a SaaS solution, you never have to worry that the version of your software is out of date. Our platform works optimally on the latest two browser versions of any browser. This security plan is designed to provide detail into the security practices and protocols at Binti.

Regulations and security requirements

Binti is compliant with the Center for Medicare and Medicaid Services, Internal Revenue Service (IRS) Policies, and is HIPAA compliant. HIPAA compliance information can be found within the business associate agreement (BAA), which can be provided upon request. Binti is strictly compliant with HIPAA, NIST Special Publication 800-63B, and commits to adhere to state and federal regulations and guidelines as well as industry standards and best practices for systems or functions required to support ADA usability requirements. We incorporate accessibility features, including WCAG 2.0 ADA requirements and Section 508 of the Rehabilitation Act, throughout the design, development, and testing processes. Binti is happy to provide a copy of our VPAT for reference.

Binti has completed their SOC2 Type 1 audit, and Binti is happy to share with customers a copy of this report for reference.

The SOC2 Type 2 audit period will cover the time period of December 16, 2020 through December 15, 2021. Our auditor will begin the attestation phase of the audit in December 2021, and we plan to provide the report to agencies in Q1 2022.

Binti is hosted exclusively in Virtual Private Clouds (VPCs) on Google Cloud Platform, which leads the industry in security and compliance and is regularly audited according to HIPAA/HITRUST, SOC2, and other compliance frameworks. More info on Google's Compliance can be found here: https://cloud.google.com/security/compliance.

Workforce Security

All Binti personnel are subject to a standard criminal background check using a BSCC-accredited, NAPBS-recognized, and FCRA-compliant vendor in accordance with California state laws.

Binti conducts background checks on all incoming new employees before their start date. We partner with Checkr and check on the following: SSN Trace, Sex Offender Search, Global Watchlist Search, National Search, and County Searches.

Upon hiring, all Binti employees must read, review and sign a copy of the "Bintipedia". Bintipedia is a company handbook to inform employees of the policies and procedures at Binti and to establish and communicate the company's expectations. It is not all-inclusive but rather offers an overview of the work environment. This document includes policies regarding Acceptable Use and our security policies.

They must confirm they have read the policies within their first two weeks of work. In addition, there is a quarterly security awareness training class.All employees are required to take a (30 minute) quarterly security awareness training class and receive a passing grade. This course covers topics such as:

- Phishing
- Spear phishing
- Malicious email
- Malicious file attachments

Binti regularly tests employees with real-world phishing campaigns to ensure that the lessons learned in the training videos have been absorbed. Binti also provides specific training for engineering and systems administrations teams that covers software engineering and systems administration security best practices.

Binti employees at onboarding are required to install Vanta, our monitoring software used to

verify several configurations, such as whether the hard drive is encrypted or a password manager is installed. Hard drive encryption using the operating systems Bitlocker or File Vault settings is required, and this is verified via Vanta. In addition asset management is performed via Vanta. Firewall is enabled on each system using the operating system's software.

Vanta is used as the anti-virus monitoring software for employees using Mac hardware, and Windows Defender is required for employees using Windows software.

Binti staff members are required to use Multi-factor authentication (MFA) when authenticating to corporate information systems. Binti staff use only hardware and software that is certified in enterprise-grade security (including full disk encryption). Our corporate premises have been audited for physical security and feature a commercial-grade intrusion detection system.

Binti customer support staff are required to complete counter-social engineering training as well as successfully complete an industry-leading Security Awareness Training program on an annual basis.

We follow the principle of least privilege when granting our employees authorization on our corporate information systems and when granting our users authorization on our products.

Employment with Binti is on an at-will basis and Binti reserves the right to discipline and/or terminate any employee who violates company policies, practices or rules of conduct. Poor performance and misconduct are also grounds for discipline or termination.

The following actions are considered grounds for disciplinary action. This list is not comprehensive, but are examples of the types of conduct this company does not tolerate. These actions include, but are not limited to:

- Engaging in acts of discrimination or harassment in the workplace;
- Possessing, distributing or being under the influence of illicit controlled substances;
- Unauthorized use of company property or assets;
- Damage, destruction or theft of company property, equipment, devices or assets;
- Removing company property without prior authorization or disseminating company information without authorization;
- Falsification, misrepresentation or omission of information, documents or records;
- Lying;
- Refusal to comply with directives;
- Failing to adequately perform job responsibilities;
- Excessive or unexcused absenteeism or tardiness;
- Disclosing confidential or proprietary company information without permission;
- Illegal or violent activity;
- Falsifying injury reports or reasons for leave;
- Possessing unauthorized weapons on premises;

- Disregard for safety and security procedures;
- Disparaging or disrespecting supervisors and/or co-workers; and
- Any other action or conduct that is inconsistent with company policies, procedures, standards or expectations.

Binti reserves the right to determine the severity and extent of any disciplinary action based on the circumstances of each case.Upon termination, an employee is required:

- to turn in all reports and paperwork required to be completed by the employee when due and no later than the last day of work;
- to return all files, documents, equipment, keys, access cards, software or other property belonging to the company that are in the employee's possession, custody or control, and turn in all passwords.

Binti will conduct an exit interview during the last week of employment.

Role-based Security Access

As a SaaS platform, role based security access is administered through login permissions. All customer data is strictly confidential to the customer. Binti staff members have only the minimum access to customer data required to perform their job functions, and all reads and writes of customer data are securely logged.

Within the application, all queries are scoped to finite sets of records in accordance to the customer's staff members roles and permissions. Binti offers comprehensive documentation thereof to ensure our business logic matches the needs of your business workflow with regards to data confidentiality. Binti has roles to grant that can be granted to an agency worker to maintain their own agency's accounts.

In addition, Binti can either do a one-time import of agency worker data given a CSV containing agency worker names and email addresses or implement Single Sign-On (SSO) of credentials. SSO eases login and simplifies provisioning and deprovisioning accounts. SSO also enhances security by reducing the number of individual credentials that users have to maintain. Given the SAML IdP Target URL and SHA1 fingerprint of agencies' certificate parameters, Binti can add this for all workers managed under the client's identity and access management environment. Binti currently supports SSO for Los Angeles County and other large agencies.

Password Management

Binti complies with NIST Special Publication 800-63-3: Digital Authentication Guidelines, which are endorsed by HITRUST.

Binti supports Single Sign-On (SSO) of credentials, easing login and simplifying provision and deprovision accounts. SSO also enhances security by reducing the number of individual credentials that users have to maintain, and simplifies administration. Given the SAML IdP Target URL and SHA1 fingerprint of agencies' certificate parameters, Binti can add this for all workers managed under the client's identity and access management environment. Binti currently supports SSO for Los Angeles County and other large agencies. Additionally, if the user in question is in a privileged role, they must also authenticate via multi-factor authentication before proceeding. For Federation, Binti supports the SAML2 protocol.

For additional security, users are prohibited from changing their passwords from within their profile. Instead, they are allowed to request a password reset, and this spawns an email password reset link that requires the user to have access to their previously verified email Account. Binti locks accounts after 5 failed passwords attempts. Agency workers will be logged out after 12 hours of inactivity. Applicant users will be logged out after 2 weeks of inactivity.

Logging / Auditing Controls

Binti maintains internal logs in our database, as well as utilizing Google Cloud's Cloud Logging system to provide a backup, auditable, trail of access logs.

In addition, we maintain an hourly read-only backup of our databases that can be used for verification against our primary database.

Binti maintains all logs for the timeline of the service agreement

Incident Management

Binti runs enterprise-grade Security Information and Event Management (SIEM) software on all of the computers in our application environment. SIEM events are fed into a centralized and secure logging, monitoring, and alerting system. The Binti Security Team handles alerts generated by the SEIM system and triages them based on the Binti Security Operations Plan. This process results in the determination that a given event was either solved and documented or declared an incident.

In the event that a security incident is declared, Binti brings in a designated trusted advisor to assist with the investigation at that time. If any customer data were found to be affected, customers (or the appropriate organizations) would be notified at the appropriate time based on local requirements.

Agency Notification Process

Severity Level	Description	Examples	Agency Notification Options
Low or	Most issues fall under	Security incident	**Contact Methods**

Medium (Class 3)	this category. These do not require someone to be paged or woken up in the middle of the night	related to agency (not connected to the Binti portal). Suspicious email from an individual who is stating they are from "Binti" and you are unable to confirm.	• Make a request or chat with a Customer Support representative at our Help Center. • Email us at help@binti.com • Call us toll-free at 844-424-6844.
High (Class 2)	These are problems where an adversary or active exploitation hasn't been proven yet, and an attack may not have happened, but is likely to happen.	Malicious access of business data (e.g. passwords, payment information, vulnerability data, etc.)	**Contact Methods** • Make a request or chat with a Customer Support representative at our Help Center. • Email us at help@binti.com • Call us toll-free at 844-424-6844.
Critical (Class 1)	The attackers were successful, and something was lost.	Applicant, agency, or child information is exfiltration (removed) from the Binti portal by an unauthorized person/group.	**Contact Methods** • Make a request or chat with a Customer Support representative at our Help Center. • Email us at help@binti.com • Call us toll-free at 844-424-6844.

Binti's Internal Security Incident Response Procedures

Once we are notified of an incident, our Customer Support team will create an internal incident response ticket and then notify the Security team in a secure chat channel of the incident. The Security team then reviews the initial findings and classifies the initial severity of the incident.

After classifying the severity of the incident, the Security team provides notification of incident Class and SLA. We will provide at least two (2) notifications:

1. First Response: An acknowledgement that the incident notification has been received by the Security team with a timeline on when we plan on remediating the incident and marking it as resolved.
2. Resolution Response: Notification from the Security team what actions were performed to

resolve the incident. If the incident includes applicant data it **will not** include personally identifiable information (PII) or personal health information (PHI). It will only provide a high level description of what steps were taken to remediate the issue.

Additional emails may be set depending on the severity of the incident until the resolution and closure of the incident.

Notification to agency or applicant is provided depending on the Severity Level of the incident. These parameters are the following:

Severity Level	**Internal Triage Process**	**Target First Response Time (SLA)**	**Target Resolution Time (SLA)**
Low or Medium (Class 3)	Ticket is created in Binti's internal ticketing system and a notification message sent in a secure Security chat room. Security Engineer and Software Engineer is assigned to investigate. Acknowledgement of incident is sent to the notifier before and after resolution of incident.	72 hours	5-10 business days
High (Class 2)	Ticket is created in Binti's internal ticketing system and a notification message sent in a secure chat channel. Security Engineer and Software Engineer is assigned to investigate. A secure dedicated incident chat room is created to communicate and notify about incident statuses. Minimum of two (2) emails about the incident is sent to the notifier before and after resolution of incident. Communication from the agency's Account Management representative (by email or by phone/internal meeting) **may** be made to provide	4 hours or better	72 hours

	additional status updates.		
Critical (Class 1)	Ticket is created in Binti's internal ticketing system and a notification message sent in a secure chat channel. Security Engineer and Software Engineer is assigned to investigate. A secure dedicated incident chat room is created to communicate and notify about incident statuses. Minimum of two (2) emails about the incident is sent to the notifier before and after resolution of incident. Communication from the agency's Account Management representative (by email or by phone/conference call) **will** be made to provide additional status updates.	1 hour or better	24 hours

Vulnerability / Security Assessment

We perform vulnerability assessments on multiple levels throughout the Binti environment:

- Static analysis is run on all code prior to release.
- A dynamic web vulnerability assessment tool is run before releases.
- A network exploitation framework tool is run on the environment prior to release.
- A software version security tool is run against the product prior to release.

Host-based network and server vulnerability assessments are performed both by Binti's hosting provider, as well as by the Binti Security Team through automated portscans conducted every two (2) weeks.

We run static vulnerability scans automatically upon every proposed code change and block changes from being integrated until we resolve issues discovered by the static scan.

Binti technical staff and a third-party security consulting firm both perform independent application, systems, and network vulnerability scans. The most recent third party comprehensive audit was conducted in October 2020 and Binti is happy to share with customers the findings of the audit.

Binti's Security staff reviews the results of vulnerability assessments -- whether performed internally or by a third party -- within one week of test completion. We review any critical findings immediately.

We address vulnerabilities based on the severity of the issues discovered, with Criticals being addressed within 24 hours, Highs within 72 hours, Mediums within 2 business weeks, and Lows within 5-10 business days.

Application Security

Binti regularly tests the security of its environment through a combination of automated tools and practices.

- Regular network security assessments
- Regular application security vulnerability assessments
- Static code analysis before every integration and release
- Criticality-based remediation prioritization

A third-party security assessment may be arranged per client request.

Application Partitioning and Multi-Tenant

Binti employs database- and application-level constraints to guarantee that all data access and data integrity is mediated by comprehensive tenant-key checks in order to achieve strict isolation between customers. The same tenant keys also unlock Google Cloud Storage objects only for users with the appropriate tenant relationships.

Anti-virus / malware controls

Binti protects our infrastructure with an industry-leading web application firewall system for all traffic entering the application. This includes HTTP(S) inspection at the application level for common threats such as Cross-site scripting, SQL Injection, Cross-site Request Forgery, and other OWASP Top 10 attacks. All web servers live within isolated Virtual Private Cloud (VPC) networks that are highly segmented from other systems on the Internet and within the Binti infrastructure. Each Internet-facing Web server is protected by its own WAF. Each system within Binti is designed and enabled to run one and only one function within the infrastructure, and superfluous capabilities are disabled.

Intrusion detection: All data is hosted on Google Cloud, which states: "Our data centers are built with custom-designed servers, running our own operating system for security and performance. Google's 500+ security engineers, including some of the world's foremost experts, work around the clock to spot threats early and respond quickly. We get better as we learn from each incident, and even incentivize the security research community, with which we actively engage, to expose our systems' vulnerabilities." https://support.google.com/cloud/answer/6262505?hl=en.

Google makes use of multiple antivirus engines in Gmail, Drive, servers and workstations to help identify malware that may be missed by antivirus signatures, as detailed in their whitepaper here: https://cloud.google.com/security/overview/whitepaper

Additionally, the Binti product uses ClamAV to automatically scan any uploaded documents before committing them to our servers. In the case a virus is detected, the user is warned and the file is not added to the Binti servers.

Network Security

Binti protects our infrastructure with an industry-leading web application firewall system for all traffic entering the application. This includes HTTP(S) inspection at the application level for common threats such as Cross-site scripting, SQL Injection, Cross-site Request Forgery, and other OWASP Top 10 attacks.

All web servers live within isolated Virtual Private Cloud (VPC) networks that are highly segmented from other systems on the Internet and within the Binti infrastructure. Each Internet-facing Web server is protected by its own WAF. Each system within Binti is designed and enabled to run one and only one function within the infrastructure, and superfluous capabilities are disabled.

Database Security

Data Classification

All data that is part of the Binti infrastructure and technology stack is classified according to the following categories:

- Public
- Internal
- Sensitive
- Restricted

Each classification level has separate requirements for data protection within the Binti environment. All PII and PHI belonging to both children and families is classified as Restricted, and receives the associated set of controls associated with that classification level.

Binti distinguishes between ordinary private data and sensitive private data. All private data is subject to carefully-audited and rigorously-tested access control. We avoid storing sensitive data except when absolutely required. When we are required to store sensitive data, it is subject to an additional level of encryption-at-rest and additional access control mechanisms. Examples of sensitive data are Personal Identifying Information (PII) and Protected Health Information (PHI).

Data Backups and Retention

Binti backs up all data in the environment at least every 4 hours, and backups are rotated according to a daily, weekly, and monthly schedule. The scheduled backups are subject to automated monitoring and routine testing. Backups are stored in a minimum of two locations at all times.

Data retention is handled according to customer requirements, with data being purged within one week's time. In the event of an expungement event, data is removed within one business day.

All backups are stored using industry standard encryption and could not be restored by an attacker even in the event of a backup provider compromise.

Data Destruction

For data destruction, there are situations in which child or family data needs to be removed from the system, e.g., a court order requiring expunging of data for those who have left the system.

To accommodate these situations, a flag is present in the database to mark whether a given record needs to be expunged. Once this flag is set, those records are then removed from both production and existing backups using an automated process.

Data Integrity Requirements

Consistent with federal standards for CCWIS (i.e. 45 CFR 1355.52 (d)(5)), Binti has developed systems to support key aspects of data integrity and quality. Based on a framework of continuous quality improvement, Binti's data quality efforts will assist agencies in formulating and updating data plans for required federal biannual reviews. Accordingly, the Binti's Data Quality Plan is organized according to the key requirements outlined by the Children's Bureau, as outlined below.

Completeness, timeliness, and accuracy

Completeness

Binti's modules are developed via extensive research in multiple jurisdictions to understand the workflows of agencies, and what data fields are necessary or available at any given phase of the process. Responses are calibrated based on user research; some fields are optional, and others required, preventing users from moving on to the next screen until the necessary information is entered. Missing fields are automatically highlighted as necessary, with the recognition that caseworkers or applicants might not have all the information at the time that the data is entered. Ongoing usage and completion of data fields are monitored at the caseworker, supervisor, manager and agency level to promote accountability and allow for setting Continuous Quality Improvement (CQI) goals for complete data.

Timeliness

Binti is designed to be used real-time and in the field, helping caseworkers do their work, rather than simply be a system of record. All the data entered into Binti and becomes immediately available for reporting and access by agency staff. We track the timestamps of items entered (but allow for adjustment of timestamps in select cases) and calculate due dates of important forms and actions by caseworkers, surfacing these in a dashboard for each worker, supervisor and administrator. Timeliness of completion of various steps in the process, as well as completion of mandated datafields, are provided in built-in reports at the caseworker, supervisor and manager level, to allow for monitoring of timeliness and setting goals for improvement.

Accuracy
Via extensive user research, Binti's has identified fields with high need for accuracy and non-duplicative data, and these are reflected in our data model. Where possible, Binti employs quick-filling dropdowns for essential data fields, combining these with adjunct text fields to provide more detail. This ensures non-duplication of data and allows for high-level analytics. On an ongoing basis, Binti examines data fields for duplicates and accuracy, and systematically reviews which data elements require additional structure or dropdown menus.

Data is consistently and uniformly collected

Binti's modules have been designed from the ground up to promote consistent and uniform collection of data from agency staff as well as private agency staff with access to the system. Common forms and required data fields are collected and integrated into the module, with careful attention that data collected for licensing is consistent in format to data that must be integrated from other systems. Staff at public and private agencies then enter data consistently and the common forms and reports populate accurately. Additional forms and data fields may be added by private agencies, but none that conflict with common data fields or forms.

Binti's carefully constructed UI also promotes consistent application of data standards, by ensuring that key terms are applied universally and that complete, clear and mutually exclusive options are selectable from dropdown menus or checkboxes. Binti systematically monitors the consistency of data, and works with agencies to update and clarify options that are unclear or misused. Trainings and guides are created or updated to include instructions on the importance of data entry as needed.

Data is exchanged and maintained confidentially

As outlined elsewhere in this document, Binti employs state of the art security and is HIPAA compliant via Google Cloud. Binti is also designed with multiple access levels for different types of users, with each user only having access to the information that they need to know in order to complete their work. Access levels are configured for each jurisdiction to ensure maximal usability while preserving confidentiality of information. In the Licensing Module, for example, Licensing workers are granted access to Home Studies as part of their duties. Many jurisdictions do not want their case carrying child welfare staff to have access to Home Studies, however, since they may contain confidential information that is not relevant to the placement decision. Access to the

Home Study is therefore restricted for case carrying child welfare staff in those agencies. On an ongoing basis, Binti reviews access levels with agency staff to ensure that access remains accurate. Audit trails of all actions taken on a case are also created and monitored to ensure accountability.

Data is supportive of child welfare policies, goals and practices

All of Binti's modules are designed to support the federal outcome indicators related to safety, permanence and well-being. Binti's Licensing Module has also been a national leader in supporting quality practice in recruiting, approving and retaining high quality caregivers. Binti's existing functionality collects data never assembled before about prospective caregivers, foster parents and resource families, greatly enhancing the ability of agencies to monitor and improve their practice. Data on a wide range of demographics, location, preferences and characteristics of both prospective foster parents is collected and can be analyzed over time to inform recruitment and retention.

Built in reporting allows agencies to examine cohorts of applicants, youth or families over time to examine outcomes and inform Continuous Quality Improvement (CQI) efforts. Extensive mapping capability allows agency staff to easily analyze geographic patterns of youth in care, available and prospective placements, etc .

Data in all of Binti's dashboards is also sortable and filterable by multiple factors, enhancing the ability of the agency to conduct checks of data quality. Filtered data from the dashboards can also be instantly downloaded in .csv format, supporting custom reports for monitoring data quality.

Data is not created by default or inappropriately assigned

Binti's has carefully designed the data fields in the modules to avoid any default settings, and creates prompts on dashboards when data is missing or has not been completed. Missing data fields are typically signified in the UI using a "?" symbol or some other signifier of missing data. Data that is pre-populated based on earlier responses is editable only by users with appropriate levels of access. Binti also avoids duplicate data entry.

Data is implemented and maintained with automated functions

All of Binti's products include an array of automated functions to assist in maintaining high quality data and prompting users to complete data entry in a timely manner.

Examples include:

- Real-time automated drop down menus for fields (such as name fields) with high probability of duplicated or misplaced records. These provide information for the user to ensure they are accurately entering information and associating it with the correct person or data object.
- Built in visual cues and warning messages/prompts for missing or misconfigured data.
- Online videos and guides for users to instantly learn about proper data entry procedures.

- Integrated dashboards for applicants and staff that provide visual representations of missing data and due dates and allow them to use one click to address the areas that require additional data entry or other actions.
- Configurable email reminders for staff and applicants that automatically remind them when documents or requirements are due and allow them to access the necessary item in Binti by clicking on the email and securely logging in.
- Real-time reports on completion of online forms and data fields so that supervisors, managers and administrators can monitor progress and develop continuous quality improvement plans for data quality.

Server and infrastructure

Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are reviewed in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. All data is stored within the continental United States.

Binti is hosted exclusively in Virtual Private Clouds (VPCs) on Google Cloud Platform, which leads the industry in security and compliance and is regularly audited according to HIPAA/HITRUST, SOC2, and other compliance frameworks.More info on Google's Compliance can be found here: https://cloud.google.com/security

Wireless, Remote and Mobile Access

Binti staff members are required to use Multi-factor authentication (MFA) when authenticating to corporate information systems. Binti staff use only hardware and software that is certified in enterprise-grade security (including full disk encryption). Our corporate premises have been audited for physical security and feature a commercial-grade intrusion detection system.

Binti is also currently working to implement MFA across agencies. Agencies have the ability to add an unlimited number of staff or applicant user accounts within Binti. There are currently 10+ access levels for staff and contracted agency users, allowing individually tailored access to the system with different access rights. If additional access levels are needed, they can be created to meet the necessary specifications. Agency-specified levels of access can create and manage new users and within Binti and their access level.

Binti employs modern tools to manage user accounts and access, and allows for updating of information and password reset by users. Binti's system allows a user to request and reset an existing password, providing a new password via email notification with a one-time link to modify the password. Strong password requirements are integrated into this process. Two Factor Authentication can also be employed. Binti has successfully integrated with a variety of Single Sign On (SSO) systems with our existing customers.

As mentioned, MFA is required for any access to Binti's internal system - including our GCP environment and our Github Code Repository. In the near future, we will be enabling VPN across all sensitive infrastructure.

Transmission

Binti has an Application Programming Interface (API) that allows for bi-directional data flow and has been used to interface with other large data systems. Binti's API is HTTPS-based, speaks JSON and XML, and conforms to RESTful principles. The API supports WebHooks in order to easily support soft real-time bidirectional data synchronization between Binti and other systems. We generate authentication tokens on request which are unique for each user. The user can make an api request along with this authentication token.

Binti stores all customer data with industry-standard AES-256 block encryption in our Google Cloud Virtual Private Cloud (VPC), and transmits data exclusively with the industry-standard HTTPS (HTTP over TLS) protocol secured by an Extended Validation (EV) certificate with an RSA-2048 key and SHA-256 signature, enforcing HTTPS at the edge and at the application level, using HTTP Strict Transport Security (HSTS). At rest the credentials are stored on a volume encrypted with AES-256, and in transit the credentials are secured with TLS with a RSA-2048 key and SHA-256 signature. Binti securely stores all data within Google Cloud. Upon written request by the county, Binti can recursively destroy complete or specific data via custom written Ruby scripts.

Binti automatically does hourly backups to ensure that data is securely maintained on an on-going basis. Furthermore, Data can also be retrieved via CSV file or via our API at any time. Binti creates hourly data backups of the data within the platform, and can retrieve copies of previous data upon request. Binti's API can be employed to extract data from Binti at any intervals to a data archive. For example, Binti's API is currently configured to provide regular back-up data to local databases in Los Angeles County and other agencies.

Continuous Monitoring

Binti runs enterprise-grade Security Information and Event Management (SIEM) software on all of the servers in our application environment. SIEM events are fed into a centralized and secure logging, monitoring, and alerting system. The Binti Security Team handles alerts generated by the SIEM system and triages them based on the Binti Security Operations Plan. This process results in the determination that a given event was either solved and documented or declared an incident.

In the event that a security incident is declared, Binti brings in a designated trusted advisor to assist with the investigation at that time. If any customer data were found to be affected, customers (or the appropriate organizations) would be notified at the appropriate time based on local requirements.

Security Audit

Security testing is performed at least annually, and takes multiple forms: A full application vulnerability assessment, user access control auditing, and information security policy review. All security testing of this type is performed by industry-leading third-party vendors. Binti technical staff and a third-party security consulting firm both perform independent application, systems, and network vulnerability scans. The most recent third party comprehensive audit was conducted in October 2020 and Binti is happy to share with customers the findings of the audit.

Change / Configuration Management and Security Authorization

All systems in the environment are built using an approved configuration policy that includes authentication, access control, data storage, data encryption, and key management.

Binti employs industry-standard tools to automate configuration management in such a way that we can easily test configuration changes prior to production, rollback configuration changes to the last known-good state in case an issue develops, and track the history of configuration over time.

These configurations include security hardening of authentication, access control, data storage, encryption, key management, etc. These configuration options are regularly checked to ensure that all instances active in the environment are secure against intrusion.

Business Continuity

Binti Disaster Recovery Plan

The Binti Disaster Recovery Plan ("DRP") establishes procedures to recover Binti operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include natural disasters, political disturbances, man made disasters, external human threats, and internal malicious activities. This DRP is maintained by the security team.

Disaster Recovery Policies

Binti performs testing of the Disaster Recovery Plan annually. The security team is responsible for coordinating and conducting rehearsals of this Disaster Recovery Plan annually. This policy and plan must be updated at least annually with additional playbooks taking into account new risks of disasters learned through testing and reenactment of past disaster incidents.

Scope of Disaster Recovery Plan

This policy includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management.

The following conditions must be met for this plan to be viable:

1. All equipment, software and data (or their backups/failovers) are available in some manner.
2. If an incident takes place at the organization's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

This plan does not cover the following types of incidents:

1. Incidents that affect customers or partners but have no effect on Binti's systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with Binti systems.
2. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Slack, and Google Cloud. The organization depends on such suppliers to employ their own continuity processes.

Notification List

In the event of a disaster, notify the people identified in the Binti line of succession.

Physical Premises Incident Response

In the event that Binti's headquarters at 1212 Broadway, Suite 200, Oakland, CA is functionally impaired, staff members will report to individually-designated off-site locations (at least one in the Bay Area and one beyond) that have been previously vetted for physical security and secure broadband access.

Binti maintains an asset registry of equipment like corporate laptops, and for each vital asset, maintains a replacement plan to procure and bootstrap a suitable substitute within 24 hours anywhere in the United States.

The Binti team's everyday operating workflow is designed not to depend on physical co-location of team members. Binti can operate our services with zero negative impact to our customers indefinitely during periods of physical distribution of the Binti team. We test our workflow and procedures by cycling employees through remote stints as well as with an annual drill during which Binti's headquarters is closed and employees report to their individual backup sites.

Binti performs annual fire and earthquake drills and compulsory trainings at our Oakland headquarters in order to ensure the well-being and safe and timely evacuation of our employees in the event of a fire or an earthquake.

Staff Incident Response

Binti's corporate organization is structured such that for every employee role there exists an alternate employee on the team that can substitute for the role in the event that an incident renders the primary employee unable to work. For particularly critical roles, Binti's plan includes two alternate team members (one of whom may be a contractor). A finite line of succession protocol is maintained in order to facilitate prompt action to resolve incidents affecting corporate officers and other key decision makers.

If the loss of the employee is determined to be long-term or permanent, Binti will use an accelerated recruitment plan to suitably fill the impacted role with a long-term replacement.

Binti's IT infrastructure and operational practices are designed to collect and exchange corporate knowledge in a secure central repository to further mitigate the impact of staff incidents.

Disaster Recovery Objectives

The objectives of this plan are the following:

- Identify the activities, resources, and procedures needed to carry out Binti's processing requirements during prolonged interruptions to normal operations.
- Identify and define the impact of interruptions to Binti's systems.
- Assign responsibilities to designated personnel and provide guidance for recovering Binti operations during prolonged periods of interruption to normal operations.
- Ensure coordination with other Binti staff who will participate in the contingency planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies. Please see Binti's critical contacts on Binti's Business Continuity Plan.

Defining Critical Systems and Services

From a disaster recovery perspective, Binti defines two categories of systems:

Non-Critical Systems

These are all systems not considered critical by the definition below. These systems, while they may affect the performance and overall security of Critical Systems, do not prevent Critical Systems from functioning and being accessed appropriately. Non-Critical Systems are restored at a lower priority than Critical Systems. Examples of Non-Critical Systems include analytics servers.

Critical Systems:

These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.

The following services and technologies are considered to be critical for Binti business operations, and must immediately be restored (in priority order):

1. Production infrastructure
2. Transit infrastructure
3. Build and deployment infrastructure

General Disaster Recovery Plan

While specific playbooks are available for specific scenarios, there are overall rules of engagement whenever a disaster incident needs to be opened.

Notification Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Binti. The notification sequence is listed below:

1. The first person to report the disaster should notify the security team lead.
2. The security team lead is to notify team members referenced above in the Notification List section.
3. Based on the damage assessment, if Binti will be unavailable to customers for more than 24 hours the security team lead will declare that a disaster has occurred and that the Disaster Recovery Procedure has been activated. The security team lead also has the discretion to activate the Disaster Recovery Procedure based on other criteria.
4. In the event customer data has been compromised, customers must be notified no later than 72 hours after the incident is reported.
5. Once the Disaster Recovery Procedure has been activated, the security team lead should notify relevant personnel and executive leadership on the general status of the incident. Notification can be conducted over chat, email or phone. The security team lead may also notify the Binti operations team if the disaster involves the Binti premises or is related to Binti employees.
6. If the Disaster Recovery Procedure has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, the security team lead and necessary team members will perform all appropriate tasks under Binti's Incident Response Plan.
7. Either the security team lead or someone they select will document who was contacted and when, and will summarize each call.

Recovery Phase

This phase covers the recovery of the application at an alternate site. If the disaster involves both Critical Systems and Non-Critical Systems, the Binti security team may prioritize the recovery of Critical Systems and proceed to the Reconstitution Phase for the Critical Systems before Non-Critical Systems have completed the Recovery Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Assess damage to affected environments, prioritizing critical systems first. Document observations.
2. If possible, back up the affected environments in a forensically sound manner. Do not alter affected systems and applications in any manner.
3. Verify that previous backups of critical databases and systems recovery points are available before moving on to the Reconstitution Phase.

Reconstitution Phase

This phase consists of activities necessary for restoring Binti operations to the original operating state (or permanently move operations to the new site or state, if necessary). If the disaster involves both Critical Systems and Non-Critical Systems, the Binti security team may prioritize reconstituting the Critical Systems before beginning reconstitution of the Non-Critical Systems. This phase consists of the following tasks, some of which can be run in parallel:

1. Begin replication of new environment using previously confirmed backups using automated and previously tested scripts.
2. Binti utilizes multiple availability zones; however, if the primary region is unavailable replicated backups should be used to create a production environment in the failover region.
3. Test new environment using pre-written tests.
4. Test logging, security and alerting functionality.
5. Verify that systems are appropriately patched and up to date.
6. Deploy new environment to production.
7. Update DNS to new environment.

Forensics Phase

This phase consists of activities related to finding out the cause of the disaster, in cases where it is not immediately apparent. Upon the disaster incident being addressed, with customer data and Binti operating infrastructure recovered and restored, it is appropriate to start the Forensics Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Ensure all logs from all systems, applications and databases involved in the incident have maintained their integrity in the centralized log repository.
2. If some logs did not reach the central log repository, ensure that missing system, database and application logs are retrieved. Pay attention to time keeping and clock settings, so logs from different sources can be reconciled.
3. If applicable, transfer data to a log analyzer or test instance.
4. Target network, system, and user action logs for analysis. Analyse all logs manually or with tools, tests, and scripts that have already been previously tested.
5. Document all significant findings in the timeline.

Retrospective Phase

A retrospective of an event such as a disaster recovery incident allows for all parties to understand what happened in a clear and blame-free manner. A retrospective meeting should occur within 7 days after such an incident has occurred.

1. All relevant parties and system owners should be identified and invited to a retrospective meeting.
2. A draft agenda and disaster timeline should be sent to everyone before the retrospective meeting.
3. Retrospectives are best facilitated with an unbiased third party who was not involved with working the incident. The facilitator should ask questions of meeting participants to illuminate the severity, impact, and any follow-ups.
4. Document the retrospective meeting.
5. Produce an incident report from the retrospective agenda, timeline, and meeting notes.

Reenactment / Test Phase

Unanticipated disasters are unlikely to have documented steps for resolution. Once an unanticipated incident concludes, it should be reenacted to analyze and document how to better respond in the future. If applicable:

1. Run a simulation of the event, as understood by the retrospective meeting notes, timeline, and report. The simulation can be run with people involved or uninvolved with the disaster.
2. While running the simulation, a pre-assigned note taker should write down ideas to prevent and mitigate a similar event.
3. After the reenactment, a new and specific disaster recovery procedure should be created.

Customer Data

Binti replicates complete backups of customer data to multiple geographically-disparate Google Cloud datacenters located in the United States. Binti's system is currently engineered to a recovery point objective of 60 minutes.

In the event of a disaster affecting our primary datacenter, customer data will be safely recovered from a secondary datacenter. Binti performs automated tests of our data recovery procedure every month.

Service Availability

Binti maintains resources in a second geographically-disparate Google Cloud datacenter in order to promptly recover service in the event of a disaster. Binti's system is currently engineered to a recovery time objective of 120 minutes.

In the event of a disaster affecting our primary datacenter, Binti will prepare our secondary system with the latest backup data, perform sanity checks, and redirect customers from the primary system. Binti performs automated tests of our service availability recovery procedure every month.

For additional information see: https://cloud.google.com/security/.

Binti Security Policy Enforcement

Disciplinary Action

Employees who violate Binti security policies may face disciplinary consequences in proportion to their violation. Binti management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Binti Security team is responsible for ensuring this plan is followed.