Agile Sports Technologies, Inc. dba Hudl

(402) 817-0060
hudl.com

600 P Street Suite #400
Lincoln, NE 68508

April 4, 2022

To Whom It May Concern:

This letter is to confirm that Agile Sports Technologies, Inc. dba Hudl ("Hudl") is the sole source provider of the following products, singularly and/or in combination:

Hudl	Sportscode
Studio	Coda
Wyscout	Hudl GamePass
Hudl Assist	Hudl Focus
Hudl Focus Indoor	Hudl Focus Outdoor
Hudl Focus Flex	Hudl Sideline
Replay	Volleymetrics

Hudl's suite is an integrated video capture, editing, and distribution solution developed for athletic teams of all levels, from youth recreational to professional. Hudl's suite is the sole source for providing an integrated solution for every state of the video analysis process.

Hudl's products are sold and supported only by Hudl. There are no resellers, agents or dealers authorized to represent these products aside from Hudl.

While there are other products available that provide some portion of similar products, there are no other like products available for purchase that offer the same integrated purpose and function, and competition is precluded for the above-named products by the existence of exclusive distribution and marketing rights.

If you desire additional information, please don't hesitate to contact Hudl at legal@hudl.com or visit our website at www.hudl.com. Thank you for your interest in our products.

Sincerely,

Matt Mueller
Chief Operating Officer
matt.mueller@hudl.com

Agile Sports Technologies, Inc. dba Hudl

(402) 817-0060
hudl.com

600 P Street Suite #400
Lincoln, NE 68508

Vendor Details:

- Legal Name: Agile Sports Technologies Inc dba Hudl
- Physical Address: 600 P Street, Suite 400. Lincoln, NE 68508
- Phone: (402) 817-0060
- Fax: (866) 851-7148
- DUNS: 94-584-6249
- FEIN: 26-0568054
- Tax Classification: C Corporation

Financial Details:

- Billing Address: 29775 Network Place. Chicago, IL 60673-1775
- Billing Email: Billing@hudl.com
- PO Policy: Purchase Orders are not required but are accepted
- Preferred PO Submissions Method: US Mail or Email
- PO Email: Billing@hudl.com

Company Information:

- Website: www.Hudl.com
- Data Service Location: Amazon Web Services
- Type of Service: SaaS and hardware
- Description of Solution: Hudl's suite is a web based and app integrated video capture, editing and distribution solution. Hudl's suite is the sole source for providing an integrated solution for every stage of the video analysis process. See attached Sole Source Letter for more information.
- Goods and Services Provided: Please see attached Sole Source Letter

Security & Privacy Overview

Summary

This document summarizes various Information Security best practices and privacy policies at Hudl. This document does not illustrate a complete representation of the Hudl environment, including controls.

Company Overview

Hudl is a leading performance analysis company revolutionizing the way coaches and athletes prepare for and stay ahead of the competition. Founded in 2006, Hudl offers a complete suite of products that empower more than 180,000 global sports teams at every level—from grassroots to professional organizations—to gather insights with video and data. Hudl's products and services include online tools, mobile and desktop apps, smart cameras, analytics, professional consultation and more.

Hudl Information Security Framework

Hudl has implemented an information security program and organization that is supported by leadership and that proactively manages information security risk & partners with the legal & privacy teams. Hudl is enhancing its program to build security & privacy by design, layering in requirements and capabilities throughout its architecture to protect its assets, supply chain, software and customer-facing services.

- Modeled after the International Standards Organization (ISO) 27001 standards. The roadmap takes into account ISO 27701, 27017 & 27018.
    - Our partner, Amazon Web Services (AWS), is certified against ISO 27001, 27017, 27018 and maintains SOC 1 Type 2, SOC 2 Type 2 & SOC 3 reports.
- Includes a comprehensive, leadership approved Information Security policy that is reviewed & approved annually for appropriateness.
- Practices defense in-depth philosophy. Multiple layers of security composed of correlated products, architectures, and methodologies.
- Incorporates SANS (Sys Admin, Audit, Network Security) Institute, NIST & ISO best practices, with a roadmap to enhance the control framework to include considerations from the Cloud Security Alliance CAIQ.
- Operates under a least privilege access model & roadmap incorporates pivoting to a zero-trust strategy.
- Hudl is compliant with PCI-DSS and maintains a SAQ-A.

Physical Security & Availability

Hudl is headquartered in the Haymarket District of Lincoln, Nebraska, with additional offices in Omaha, Nebraska; Boston, Massachusetts; London, United Kingdom; Sydney, Australia; and Mumbai, India. Hudl services & data are powered by Amazon Web Services (AWS). Data is primarily stored in AWS's US-East (North Virginia) "us-east-1" region; videos are stored within Amazon regions close to the uploading origin. While most of our infrastructure is located in the United States of America, we utilize AWS locations inside the E.U., as well as within Third Countries protected by US approved Standard Contract Clauses.

Office locations are secured 24 hours a day, 365 days a year, with access solutions that restrict onsite and specific room access to personnel authorized based on their job function. Access is logged and available to support incident investigation if required, including staffed reception desks & video surveillance.

Security Incident Response & Escalation

Hudl has implemented formal processes for monitoring the security & availability of its services. The information security program relies on alerts, automation & escalation procedures to notify personnel outside of core business hours. Alerts are configured to notify the appropriate team to take action according to standard procedures. In the event of a suspected incident & reasonably suspected breach, Hudl will use commercially reasonable efforts to contain, mitigate and resolve the incident as well as put in place additional controls to prevent further incidents of a similar type.

Hudl will notify data controllers without undue delay, typically within 48 hours or sooner, once an incident has been confirmed to impact scoped data. All of Hudl's third party contracts comply with current data protection legislation and explicitly state security requirements within the service provision.

Data Security & Availability

An information security policy has been written and communicated to users that addresses physical and logical considerations, defines user IDs, passwords, and account management procedures. The policy is available to Hudl employees for reference when administering security to internal resources and customer environments. The program is designed to protect Hudl from internal and external threats, loss, and unauthorized disclosure. The security & privacy teams are focused on managing risk as a continuous cycle seeking to manage and build effective security and privacy controls, quickly detect & respond to incidents, and test the

effectiveness to maintain a healthy operating risk and compliance posture for Hudl and its customers.

Hudl has implemented policies and procedures for infrastructure and software hardening and configuration. Hudl laptops & infrastructure are scanned for known vulnerabilities on a periodic basis. Vulnerabilities are prioritized for remediation and applied as part of the development lifecycle process. Endpoint Protection & Extended Detection & Response software is installed on Hudl devices. Access requests for new employees are documented within the ticketing system and permissions are role-based. Access to Hudl resources is granted based on a user's job function and responsibilities. Administrator access is restricted to appropriate personnel based on job function and responsibilities. If access is no longer necessary, it is removed within 72 business hours.

Access to Hudl resources is restricted to Hudl personnel through the use of user IDs, passwords and multi-factor authentication. Certain sensitive or confidential resources are only accessible with an additional Virtual Private Network (VPN) connection, transport layer security (TLS), or other encrypted communication system.

Hudl provides Information Security & Data Protection training upon hire and at least annually; attendance & completion is tracked through the Learning Management System (LMS). Hudl also performs background screening, testing & reference checking as part of the hiring & onboarding process. All personnel, including third parties when applicable, are subject to confidentiality agreements.

A formal Enterprise RIsk Management program has been established to manage organizational risks across all business units & functions. A zero-trust aligned strategy has been established to guide the maturity of ISO 27001/2 aligned controls within the Information Security Management System (ISMS) and any in-scope domains. Hudl supports no less than transport layer security (TLS) 1.2 for data encryption in-transit over public networks and is on track to encrypt all data at rest within the AWS environments meeting FIPS 140-2 Level 1 standards.

The software development life cycle includes several functional, non-functional and security testing requirements. An enhanced security (S-SDLC) policy is in development to refine and mature requirements spanning threat modeling, third party library risks, OWASP concerns, more formalized static/dynamic code testing and developer training. Change management and tracking is tied to role-based access and repositories are monitored.

Hudl maintains business-continuity-like processes fronted by dynamic rerouting of traffic and load balancing within AWS. Failover and load-testing scenarios are periodically tested. AWS is responsible for large scale system failover, such as DNS. Hudl performs regular testing of its platform to ensure the data controller's service meets the agreed SLAs and SLOs.

Customer Data

Hudl's security program is designed to protect against the accidental or unauthorized damage, loss or access of any Customer Data. Hudl has implemented administrative, technical, and physical safeguards designed to ensure the confidentiality and integrity of Customer Data. In addition to the controls implemented by Hudl, Hudl leverages industry-leading providers that implement industry best practices for the protection of data.

Hudl limits access to Customer Data to those Hudl Personnel who need to access the Information Systems in support of the Software or Services, and such personnel are required to sign agreements with confidentiality protections as part of their employment. Hudl treats all Customer Data as the customer's confidential information. Due to the nature of Hudl's products and the nature of a SaaS product and supporting environment, Hudl does not apply customer-specific data classification schemes to Customer Data; rather, Hudl classifies all Customer Data at its highest level of data classification.

Hudl can accommodate secure erasure or destruction of all media that contains Customer Data. Hudl will select the appropriate industry-standard procedures, such as NIST SP 800-88. All Customer Data, including any backups of Customer Data, are planned to be encrypted at rest using algorithms that meet or exceed industry standards.

Authentication & Authorization

Hudl uses industry standard techniques designed to restrict access to and prevent unauthorized use of its Information Systems. Hudl requires the use of individual user accounts to maintain the integrity of audit trails. Access to resources is subject to the roles an employee is fulfilling; password complexity requirements and minimum key lengths are enforced for all identities. Hudl also leverages multi-factor authentication for access to all systems.

Hudl follows the principle of least privilege | system owners maintain access control policies, procedures and documentation for each system, including the privileges assigned to users and

groups. Where possible, user and group management is centralized using single-sign on systems.

Change Management

All changes to Information Systems by Hudl personnel in production environments, including network and other infrastructure, are authorized, tested & monitored. Changes to software undergo peer review and quality assurance testing prior to release. Where possible, changes are performed through configuration management and automation/infrastructure as code.

Endpoint Security

Hudl employs a defense-in-depth strategy for endpoint security that is designed to block access to known-malicious sites and applications, as well as monitor for indicators of compromise. All endpoints are centrally managed and configured through mobile device management to ensure compliance with established baseline configurations. All endpoints are configured with full-disk encryption. Hudl leverages anti-virus/anti-malware endpoint detection & response solutions on all endpoints.

Business Continuity & Disaster Recovery

Hudl maintains business continuity and disaster recovery plans designed to minimize the impact of potential threats to business operations. Hudl maintains multiple availability zones to provide redundancy in operations and enable high availability of the Service. Hudl customers can view updates on: https://status.hudl.com/.

Network Security

Hudl employs a defense-in-depth, zero-trust aligned strategy for network security including the use of host-based and web application firewalls, segregation of development, test & production environments, and access control lists/security groups between virtual private clouds (VPC). AWS provides distributed denial-of-service (DDoS) protection that ensures the uptime and availability of resources. Encryption in transit over public networks is minimum TLS 1.2, with support for TLS 1.3.

Logging & Monitoring

Hudl monitors the Information Systems as well as the underlying infrastructure for security incidents during normal business hours; The information security program relies on alerts, automation & escalation procedures to notify personnel outside of core business hours. All systems generate security and operational logs, which are forwarded to the centralized logging system and monitored for anomalous activity that generates alerts for further investigation.

Risk Management

A formal Enterprise RIsk Management program has been established to manage organizational risks across all business units & functions. A zero-trust aligned strategy has been established to guide the maturity of ISO 27001/2 aligned controls within the Information Security Management System (ISMS) and any in-scope domains. This includes ongoing risk identification and assessments of people, processes, data, and technologies to identify confidentiality, availability or integrity risks; their operational, business interruption, financial, reputational, legal and/or regulatory impacts; as well as the likelihood of occurrence.

Vulnerability Management

Hudl follows a risk-based methodology leveraging relevant industry standards, such as CVSS, to prioritize security issues based on their impact severity and likelihood of exploitation. Hudl aims to release patches or remediate an issue in a reasonable period of time commensurate with the results of the risk assessment. Generally, higher-impact issues will be prioritized and fixed sooner than lower-impact issues. However, the exact amount of time required to fix a vulnerability is unique to each finding and depends on a set of factors, including the complexity of the issue, the number of components impacted, and any third party dependencies.

Hudl's intent to discover and remediate vulnerabilities in its suite of products prior to release. In order to accomplish this, Hudl utilizes industry-standard techniques as part of its software development life cycle. Such techniques include peer code review prior to merge; static application security testing (SAST) of code changes; scans of build artifacts; and scans of third-party libraries and dependencies for known vulnerabilities.

Hudl's vulnerability management program is also designed to detect vulnerabilities at all layers of the Information Systems using industry-standard tools and to track identified vulnerabilities until remediation. Hudl subscribes to notification channels for its vendors as well as industry feeds for vulnerabilities. Hudl also regularly engages qualified third parties to perform independent assessments of source code, products, and infrastructure.

Privacy

All data that Hudl sends out of the EU/EEA is sent to countries with an EU adequacy status or to organizations with signed EU Standard Contract Clauses. Hudl transfers data between its group of companies, for which the international transfers of EU/EEA data are detailed within Hudl's Intra-Group Data Transfer Agreement, which itself includes the required EU Standard Contract Clauses. All Hudl data transfers to the US are TLS encrypted and generally consist of

insensitive personal data. Hudl therefore believes the risk of government surveillance to the privacy of transferred personal data to be very low. Additionally, Hudl will only provide personal data to applicable law enforcement authorities when under strict legal compulsion. When permitted by applicable law, law enforcement and exigencies of time, Hudl will notify its customers of any such legal requests involving their personal data.

Hudl is primarily a data processor, and as such acts under the direct instructions of the data controller who maintains complete responsibility to establish a lawful basis for processing the data subject's data, e.g. that of an athlete. Hudl's data processing meets its GDPR requirements and Hudl adheres to the six principles of lawful processing of Article 6 of the GDPR. Hudl's internal processes provide clubs with the ability to export, rectify and erase data should they need to service such a data subject request.

Hudl processes data on behalf of the club to provide the services. This data relates to the team, its athletes, their contact information, videos, photos, analytical data and messaging. This may include name, home and email addresses, phone number, school (name, city and state), graduation year, GPA, ACT/SAT scores, transcripts, parent/guardian information (name, relation, email and phone), age, birth date, photograph, height, weight, jersey number, Twitter handle, sports position, performance scores (40-yard dash, agility shuffle, power ball, vertical jump), speed and strength information, sports awards, sports videos featuring the athlete, and other athlete profile information.

Hudl retains customer data for the length of the service agreement with Hudl and as defined in the customer's contract. Hudl provides Sportscode software which provides local processing of data. No personal data is sent from the Sportscode software to Hudl. In turn, Hudl itself does not process personal data of the club through this software product.

Appendix A - Quick Facts

Headquarters

Agile Sports Technologies, DBA Hudl

600 P. Street, Suite 400

Lincoln, NE 68508 USA

+1-402-817-0060

Chief Information Security Officer (CISO) details:

Name	Rob LaMagna-Reiter
Email	security@hudl.com
Post	Chief Information Security Officer; 600 P St. Suite 400; Lincoln, NE 68508 USA
Phone	+1 402-817-0060 (Lincoln HQ number)

Data Protection Officer (DPO) details:

Name	Carl Gottlieb
Email	dpo@hudl.com
Post	Data Protection Officer, Hudl UK, Ltd, Suncourt House 2nd Floor, 8-26 Essex Road, London, N1 8LN, United Kingdom
Phone	+1 402-817-0060 (Lincoln HQ number)

EU Data Protection Authority Registration

Our UK subsidiary, Hudl UK, Ltd, is registered in England and Wales under registration number 06962812, with registered office at Suncourt House 2nd Floor, 8-26 Essex Road, London, England, N1 8LN. Hudl UK, Ltd is a registered Data Controller with the UK Information Commissioner's Office (ICO), number ZA326152. Hudl's Privacy Shield Certificate is here.

Privacy Policy

Hudl's Privacy Policy is available here.

Resources

Amazon Web Services

- Hudl case study
- Hudl blog post
- AWS security overview
- AWS ISO certification
- AWS SOC 3
- AWS SOC 1 & SOC 2

Appendix B - Frequently Asked Questions

The following represents a list of frequently asked questions. Contact your account management team or customer support if you require additional information.

- Does your company have a position or organization responsible for overseeing the company's overall security program?
    - Yes, Hudl has internal information security that is responsible for ongoing operations, maturity, engineering, architecture, as well as governance, risk and compliance
- Could you describe the service Hudl provides?
    - Hudl is a web-based sports analysis software that allows teams to upload and analyze video as well as communicate within their team(s) and also exchange video with other teams.
        - Cameras, such as the Focus Indoor, Focus Outdoor, or Focus Flex automatically captures every event, uploads the footage to Hudl and supports livestreams.
    - Hudl Sportscode is a fully customizable performance analysis solution that can connect with Hudl's collection of online, offline and real-time video and data analysis tools to create a streamlined experience.
    - Wyscout is the world's biggest library of global football video and data, available in one platform. It also supports scouting, match analysis & transfer dynamics.
- Is Hudl's platform accessible over the Internet?
    - Yes, Hudl's solution is considered Software-as-a-Service (SaaS).
- Are mobile applications available?
    - Yes, an iOS or Android application is available for Hudl.
- Is my data co-mingled with other Hudl customers?
    - No, Hudl's backend systems support a segmented, multi-tenant environment in AWS. Data is not co-mingled.
- Does the company meet responsibility for compliance legislation (for example, NJ ID Theft, etc) and/or third-party requirements such as HIPAA, GLBA, etc?
    - Hudl stores limited personal information, including name, e-mail address, phone number and other pieces of contact information uploaded in the platform. Hudl is not subject to HIPAA or GLBA. Hudl conforms to geographic-specific privacy and/or security requirements, such as GDPR.
- Does Hudl have a formal Security Policy?
    - Yes. It is reviewed annually for necessary changes and made available to all Hudl employees.

- Does Hudl have a formal security incident response policy?
    - Yes, Hudl maintains a formal security incident response policy and it is reviewed/updated annually.
- May I request a copy of Hudl's security or incident response policies?
    - No, Hudl's internal policies are not authorized for external distribution.
- Does Hudl have an Acceptable/Responsible Use policy?
    - Yes
- Does Hudl have a Privacy Policy?
    - Yes - Please see here
- Does Hudl have documented standard processes for change management?
    - Yes; processes are being updated to better align with ISO 27001/2 requirements
- Does Hudl support Single-Sign On?
    - Not generally; if Single-Sign On is a requirement, please work with your account management team to discuss options. Single-Sign On is a feature currently under development with no committed release date.
- Does Hudl require unique accounts for access?
    - Yes
- What password complexity requirements does Hudl support?
    - Hudl permits users to change their password at any frequency. Currently, there is no minimum requirement. Hudl uses a complexity formula that meets NIST minimum standards.
- Are inactivity sign-outs available?
    - Yes, inactivity sign-outs are set for 1-hour
- How are privileged/administrator accounts handled?
    - Team Administrators perform administrative functions on coach/video coordinators, etc accounts.
- Are audit logs available in the event of an incident investigation?
    - Yes - login, logout, actions performed & source IP are available. This information is only available to authorized contacts.
- Are regular security assessments performed on your environment?
    - Yes, annually Hudl performs traditional fully-scoped penetration tests. Real-time and monthly, Hudl performs vulnerability scanning, external application scanning and threat analysis. All findings are validated and prioritized for resolution according to our vulnerability management program.
- Does Hudl maintain separate development environments?
    - Yes, Hudl maintains separate environments for development, testing & production, as well as role-based access into each environment.
- How will customer information be disposed of when the contract is terminated?
    - Customer information is securely erased and rendered unrecoverable if customer's choose to terminate their contract.