Information Security Content for OCP.

What is OCP?
The OCP is the new Online Claims Platform. It digitally connects certified FSC® suppliers and customers so that claims for FSC-certified products can be swiftly confirmed as accurate by both trading parties. As products move down the supply chain, their FSC certification can be assured. This system will enhance the integrity of the FSC brand.

FSC foresees that the use of the OCP could significantly reduce the administrative burden of being FSC certified. Thus, we are identifying the possible ways larger parts of the CoC standard can be automatically met for certified organizations that fully integrate the OCP. These changes would lead to saving time on administration and auditing processes, while building a more robust FSC system.

If you would like more detail, please visit ocp-info.fsc.org.

What data does OCP collect?

OCP will be populated with your organizations publicly available certificate data as published on info.fsc.org.

Users of OCP can locate and connect to their suppliers or customers and record data for FSC certified goods traded between the parties.

Information entered on traded goods is limited to a transaction identifier, date, claim type, product type, traded volume, description & species where applicable.

OCP does not collect any financial or proprietary information.

If you would like more detail you may like to check out the OCP Help Site, specifically, Data fields in OCP.

How do we keep OCP information secure?
We are committed to protecting the information assets we keep for our customers, partners as well as our own information assets so we have set objectives for information security management. This includes certification to ISO 27001 by Q3 2014. ISO 27001 is a globally recognized security standard that provides a guideline of the policies and controls that an organization has in place to secure data. The standard sets out internationally agreed upon requirements and best practices for the systematic approach to the development, deployment and management of a risk/threat based information security management system.

What this means in practice is:

HF operates and maintains an information security management system (ISMS) to control its information assets appropriately. This includes classification of all assets with clear guidelines on how information can be handled.

HF has implemented and applies the internal policies and procedures that support the ISMS. As part of a management system it is independently audited by Certification Europe at least annually and by external security specialists to ensure compliance.

Security Awareness training is part of our induction and ongoing staff development processes, ensuring our team are aware of the policies and procedures in place to safeguard the security of information.

We implement human, organizational and technological security controls driven by the ISMS controls (Statement of Applicability) to protect information assets from unauthorized access, leakage, modification, theft / loss, denial of service attacks, or any other threat.

We take breaches seriously and have a formal incident management process to identify, contain and recover from a security incident should one occur, with a bias to over communication and commitment to inform our users.

HF through its ISMS makes efforts to rapidly locate the root cause, keep damage to a minimum and prevent the recurrence if an incident posing a threat to information assets should occur.

HF complies with all legal/regulatory and contractual requirements related to information security and adopts UK Law guidelines, industry standards and best-practice for information security.

HF continuously reviews and improves these activities through internal audits, the exercising & review of our procedures.

In line with our ISMS controls the detection and resolution of security weaknesses include the use of periodic security penetration testing of the OCP, which is undertaken by an independent third party, the NCC Group.

HF delivers its services based on the following legal/regulatory framework

- Telecommunications Act.
- Data Protection Act.
- Contracts with Historic Futures customers.
- HF utilize third party legal expertise for advice.

If you would like more detail you may like to check out ISO27100.

What happens if something goes wrong?

We take breaches seriously and have a formal incident management process to identify, contain and recover from a security incident should one occur, with a bias to over communication and commitment to inform our users.

HF through its ISMS makes efforts to rapidly locate the root cause, keep damage to a minimum and prevent the recurrence if an incident posing a threat to information assets should an incident occur.

All incidents are graded depending upon their severity in line with our ISMS risk management procedure. All incidents with a magnitude of Priority 2 or higher will be posted to ocp-status.fsc.org a public, independent website. (Currently hosted at http://ocpstatus.tumblr.com/) OCP uses are also provided with access to our ticketing system enabling users to report any problems or incidents arising.

Below are some of the most frequently asked questions by our users. If any user notices anything suspicious, please contact us via our support desk by clicking here.

STANDARDS AND CONTROLS

What security standards & controls are in place?

HF management is committed to protecting the information assets it keeps for our customers, partners as well as our own information assets and has set objectives for information security management. This includes certification to ISO 27001 which is a globally recognized security standard that provides a guideline of the policies and controls that an organization has in place to secure their data. The standard sets out internationally agreed upon requirements and best practices for the systematic approach to the development, deployment and management of a risk/threat based information security management system.

Do you adhere to SAS 70?

HF has implemented an ISMS to the international security management standard ISO 27001, this standard has a number advantages over a SAS70 security statement. The standard specifies security management best practices and has comprehensive security controls. Certification to the standard requires HF to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities.
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks.
- Adopt an overarching management process to ensure that the information security controls meet our information security needs on an ongoing basis.

The key to the ongoing certification under this standard is the effective management of a rigorous security program. The ISMS requirement defines how we continually manage security in a holistic and comprehensive way. The ISO 27001 certification is specifically focused on the HF ISMS and measures how our internal processes follow the ISO standard. The annual certification by the third

party accredited independent auditor confirms that our processes and controls are operating in alignment with the 27001 standard.

SOC 1/SSAE 16/ISAE 3402 (formally SAS 70) is an auditing standard used to enable an independent auditor to evaluate and provide an audit statement on a company's control objectives and activities. Globally ISO 27001 is being utilized by more companies to provide business assurance as it requires ongoing management and enhancement of risk and controls through a continuous improvement model unlike the former SAS70 statement.

The commitment for an ISMS by HF is summarized in the following table based on the differences between each standard.

Methodology	ISO 27001	SOC 1/SSAE, 16/ISAE 3402
Intended Use in Business	Management requirements	Audit guidance for minimum requirements
Assurance	International certification	Service auditors report
Scope	Business focus for an and all forms of information and/or systems	Financial focus (statements and related systems)
Stance	Proactive	Reactive
Risk	Identify, measure and remediate	Maximize risk and then reduce
Control Definition & Measurement	Each control is defined and measured as a requirement of an ISMS	Type 1 audit report provides findings but does no cover testing or effectiveness of controls. The testing of controls is included in a Type III audit report.
Continuous Improvement	Mandatory updates with plan-do-check-act	Not included

What security policies, standards apply?
HF has developed policy and procedures based on industry and vendor best practices to protect the information assets it keeps for our customers, partners and our own information assets. The communications and operations management is planned for and deployed with regard to the security of HF information assets and the operations of the whole information processing environment.

The policy and procedures set standards for the following:

- Information security policy
- Clear desk and clear screen policy
- Asset disposal policy
- Cryptographic policy
- Access control policy
- Acceptable use policy
- Mobile computing policy
- Network services policy
- Information exchange policy

- Business continuity policy
- Incident management procedure
- Information classification procedures
- Risk management procedure

Internal audit procedure:

- Document and records control procedure
- Corrective actions procedure
- Preventive actions procedure

Each policy and procedure supports the required controls as set out by the ISO27001 standard Statement of Applicability and how HF manages its information assets.

Who audits the HF ISMS policy?
Certification Europe.

HF has a letter of attestation in November 2013 by an external security consultancy providing our security posture and commitment that meets the intent of ISO 2700 leading to certification.

An external review has been completed by external security company CQR in 2013 against ISO 27001 and covered:

- Management System Documentation
- Risk Management
- Document & Records Management
- Training, Awareness & Competence
- Incidents, Corrective and Preventive Actions
- Business Continuity Planning
- Control Implementation

HF completes penetration testing on effectiveness of technical controls.

HF is going through a set process to gain certification by an independent body Certification Europe. The certification assessment has two phases, Stage 1 is scheduled for May and completed on site by the auditor to determine that the HF system has met the requirements of the standard and is capable of being certified. Stage 2 follows after Stage 1 and is an audit of the effectiveness of the system. Both stages must be completed to become certified. Stage 2 is scheduled for June 2014 and certification is achieved after this time.

Each stage is completed on-site and includes:

- Observation of process / activities and staff
- Review of documents, controls and records
- Discussions with site management and staff

The certification body provides ongoing surveillance audits each year based on a sample basis of the HF ISMS to ensure HF maintain certification.

Who conducts Penetration testing on OCP?
In line with our ISMS controls periodic testing of OCP is undertaken by an independent third party, our current service provider is NCC Secure.

DATA AND STORAGE

Where is my data stored?
The data is hosted with Amazon Web Services in their European data centers based in Dublin, Ireland.

The data center is owned by Amazon Web Services and is a subsidiary of Amazon.com, Inc. or its affiliates ("Amazon.com"). The Amazon Group companies have certified that they adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U.

If you would like more detail you may like to check out Amazon's security information.

Have have you assessed risk associated with offsite storage?
HF used an independent security company to conduct a risk assessment for the hosting solution with the key objective to provide HF with a level of assurance that the hosting solution provides effective and appropriate security controls for its information and that it does not introduce risk through the use of off-site processing and storage.

Amazon EC2 has compliance to regulations, standards and best-practices to maintain security and data protection to provide a level of assurance of protection. These include ISO27001, HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, FedRAMP(SM), DIACAP and FISMA, ITAR, FIPS 140-2, CSA, MPAA.

The system will run concurrently across two Amazon availability zones (the equivalent of two different data centers). (Spring 2014 only one data center currently operational)

ACCESS CONTOLS

Who can access to our OCP data?
Certificate data can be accessed by the account holder & account administrators, users permissions is managed by the OCP account administrator from within the OCP service.

Claim data can be viewed by both trading parties in the process of confirming claims.

Amazon AWS administrators do not have access to customer instances, and cannot log into the guest OS.

Historic Futures, FSC support & Certifying Bodies do not routinely have access unless granted by the account administrator.

If you would like more detail you may like to check out the full Terms and Conditions.

As stated in the Terms & Conditions: "FSC reserves the right to authorize Historic Futures to monitor, review and/or retain at all times any activity deriving from Authorized User's account exclusively in order to ensure a well-functioning system and / or disclose of any information insofar as necessary to abide by any applicable law, regulation, legal process, threatened legal action or official governmental request." So, this really means that if a CH has a question / problem with the OCP and needs to share any of their OCP account information with support staff, then that's when FSC may have access to their account – for the sole purpose of helping the CH after the CH requests this.

What are Amazon's physical security controls?
Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
Incident Management

What procedures are in place to protect against unauthorized access of the system and physical access to the data centers?
Access to HF information assets is on a need basis in order to reduce the risks associated with misuse, such as alteration, destruction and unauthorized dissemination of information. The HF information security policy sets baselines for Access Management covering:

- User registration and identification

Roles and responsibilities

- Approval of access by the Owner
- User authentication
- User authorization
- Privilege management
- Operating System control
- Network access control
- User password management
- Review of access rights
- Remote access

INCIDENT MANAGEMENT AND DISASTER RECOVERY

How is back-up and restore arranged in case of outage, fire, molest
The master databases are backed up hourly to Amazon S3. We keep a rolling history of 10000 backups.

Can OCP switch between data centers?
The OCP has been designed to operated across multiple data centers, the loss of a single data center should not result in downtime.

What is your disaster recovery plan (DRP)?
The OCP system is built from generic virtual machines and designed so that the loss of any single machine will not result in downtime.

Each server is built from a standard and can be rebuilt, on demand within minutes.

How are performance levels monitored?
The independent service provided by Pingdom.com is used to monitor system uptime and response time from a number of locations around the globe. FSC has an SLA agreement in place with Historic Futures governing system response times.

What is the uptime performance target for the OCP service?
The uptime / availability SLA agreed is 99% measured monthly.

What procedures are in place to protect against viruses, malicious codes, and unauthorized software?
The HF information security policy sets baselines for monitoring mechanisms to identify security trends and detect anomalies. Anomalies are reviewed to determine if they are indicative of a security event. Events are reported, investigated, escalated, and corrected to enable a rapid return to normal business operations. The process covers Event detection and response and vulnerability management.

What procedures exist to protect against software corruption and data loss?
When HF proposes new systems or changes to existing, the security aspects of the systems are included in analysis and specification. These specifications cover automated and manual security measures which are supported by a risk assessment.

The baselines include:

- Security of system files
- System planning, acceptance and acquisition
- System development
- Data validation

HF use business continuity planning (BCP) for its business resources so as to minimise the effect that a disaster or business disruption. BCP within HF provides documented processes to enable the business process to continue in the event an asset is destroyed or unavailable. Disaster re-

covery planning (DRP) is the process to recover an IT asset after an event has made the asset unavailable to the business.

The baselines for business resiliency include:

- Planning
- Testing
- Maintenance
- Awareness
- Backup and recovery

How should I report a security issue?
Through our ticketing system: support@ocphelp.zendesk.com

Do you have a designated security Officer / Privacy Director?

- In line with ISMS requirements Historic Futures has a designated security owner.

In the event of a crisis how and when will the FSC communicate with me?
All incidents are graded depending upon their severity in line with our ISMS risk management procedure. All incidents with a magnitude of Priority 2 or higher will be posted to ocp-status.fsc.org a public, independent website. (Currently hosted at http://ocpstatus.tumblr.com/)

Will I be notified of all privacy related problems and incidents (e.g., privacy data breach) involving and / or impacting my data?
HF operates an Incident management procedure which is followed whenever a security or privacy incident occurs. The response varies appropriately with a strong bias toward over-communicating.