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.

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. OCP developers make 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.

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.

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

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.

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 operate 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

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?
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.

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

In the event of a crisis how and when will the FSC communicate with me?
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/).