.scot Compliance Procedure

The .scot Registry, with the assistance of its backend registry provider CORE Internet Council of Registrars, will establish, thorough and effective methods to prevent abuse of .scot domain names, .scot registrant data or the associated infrastructure, as well as to mitigate any impact from such abuse (should it occur despite the preventive measures). In order to achieve this, the .scot Registry is committed to deploying extensive organizational and technical measures. The most salient examples of these measures are described below.

1. Rapid Takedown Policy for Cases of General Malicious Activity

The .scot Registry has committed to closely collaborate with law enforcement authorities and security agencies in order to take quick action in case a .scot name is reported to be involved in malicious activity. For this purpose, a Rapid Takedown Policy is established that:

1. identifies cases of malicious activity;
2. defines ways for the registry to be notified of such activity (e.g. via a dedicated website, e-mail address or phone hotline);
3. defines clear and consistent procedures to quickly stop the malicious activity (after the activity was confirmed and impact of the measures has been assessed),
4. defines related service levels (e.g. with respect to the maximum time the registry may take to respond to takedown requests). This time limit will never exceed 15 business days in the case of less urgent cases, and not exceed 24 hours in the most urgent cases such as phishing,
5. defines rules regarding the notification of involved parties (registrant, administrative contact, technical contact, registrar, informant),
6. defines ways to appeal against any measures taken (through the general Eligibility Restrictions Dispute Resolution Procedure as is the case for all appeals against Registry decisions, but with panelists that are specialized in Security and Malicious Conducts).
7. defines how cases covered by the policy need to be documented and reported. In this context, cases of malicious activity may include (but are not limited to):
    a. wrong, invalid or harmful DNS setup (e.g. pointers to false IP addresses),
    b. use of trademarked or otherwise reserved names without proper rights,
    c. use of the domain in actions that affect the stability and security of the Internet (e.g. in Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks or botnets),
    d. use of the domain for the distribution of malware (such as computer viruses, worms, Trojan horses, spyware or rootkits),
    e. use of the domain for phishing or scamming,

f. use of the domain for spamming (affecting e-mail or other forms of electronic messaging).
g. maintaining invalid registrant contact data in the domain.

Where applicable, the policy includes metrics and thresholds for finding quantitative indications of malicious conduct.

Procedures to stop malicious activity may include (but are not limited to):

1. notifying the domain's sponsoring registrar, specifying a deadline until which the activity needs to haveceased,
2. notifying the domain's registrant, administrative or technical contact directly (again specifying a deadline until which the activity needs to have ceased),
3. locking the domain and putting it on hold in order to prevent changes to the domain and remove it from the .scot zone ("takedown"),
4. deleting the domain name and blocking it from further registration if need be. Escalation rules (defining which steps are to be taken in which order and conditions for moving on to the next, more drastic measure) are part of the policy.

Since removing a domain name from the .scot zone usually has serious consequences (such as rendering websites and e-mail addresses utilizing the domain name unusable), the .scot Registry will, in accordance with the policy, exercise extreme caution with regard to any takedown decision.

At the same time, the .scot Registry is aware that malicious activity potentially affects a large number of Internet users, which sometimes warrants drastic measures. The Rapid Takedown Policy aims at finding appropriate measures, taking the interests of all involved parties into consideration. The Rapid Takedown Policy will be announced to both .scot registrars and .scot registrants and be part of the Registry-Registrar Agreement (RRA) and the .scot registration terms.

2. Rapid Takedown Policy for Cases of Phishing

The .scot Registry will work closely with all CERTs and CSIRTs in the relevant area to develop an Anti-Phishing-specific simplified procedure. The goals will be to:

1. get all seventeen UK CERTs and CSIRTs (at least, but open to other CERTs) accredited as Authorized Intervenors),
2. develop criteria and checklist for domain names eligible for Rapid Suspension,

3. develop secured communications method between Authorized Intervenor and Registry, including an Affidavit form.

Names reported by Authorized Intervenors will be suspended in less than 4 hours. This system should expand to a global Authorized Intervenors list. In this regard, the .scot Registry will work with the Antiphishing Working Group and other initiatives in order to develop and complete their proposed Accelerated Takedown proposal, which is still in beta stage.

3. Single Point of Contact for Abuse

To ensure that the .scot Registry gets notified of any cases of abuse as quickly and as easily as possible, an area of the public website operated by the .scot Registry for the .scot TLD will be dedicated to the reporting of such cases.

The respective web pages establish a single point of contact where abuse cases can be reported via a simple web form. An e-mail address and a phone number will also be provided as alternative means of communication.

Every case reported will raise a high-priority ticket within the .scot support staff's ticket system, to be examined immediately and treated in accordance with the Rapid Takedown Policy (and the other Compliance Procedures related to Eligibility and Use, and Trademark Claims).

4. Prevention of Domain Name Tasting or Domain Name Front Running

The life cycle of a .scot domain name includes a 5-day Add Grace Period (AGP) during which a newly created domain name may be deleted with a refund of the domain fee. This is common practice and corresponds to the policies of almost all existing generic top level domains.

However, in the past the Add Grace Period has been abused for practices such as domain name tasting and domain name front running.

Domain name tasting means that domains were created simply for the purpose of testing whether revenue can be generated by e.g. creating a web page with advertisements for the domain; if this was found feasible within the first few days, the domain was retained, otherwise it was deleted within the add grace period for a full refund, i.e. the domain was ″tasted″ for potential revenue without any payment to the registry.

Domain name front running refers to the practice of pre-registering domain names somebody has merely expressed interest in (e.g. by searching for them on the Whois web front-end of a registrar) with the purpose of reselling the domain to that person (at an inflated price) afterwards;

again, the Add Grace Period has been abused for this purpose since a registrar could do that without any cost (if the unsold domain was deleted before the end of the add grace period).

In 2008, ICANN introduced the so-called ″AGP Limits Policy″ which addresses these and other issues resulting from the Add Grace Period. The .scot Registry will fully implement this policy by restricting Add Grace Period refunds to registrars according to the limits specified by the policy. At the end of every month, the registration system′s billing module will determine every registrar′s net domain adds and check whether the add grace period refunds granted during that month exceed the permissible number according to the policy; if this is the case, additional charges to the registrar′s account will be initiated to effectively revert the excessive refunds.

Any exemption requests by registrars, whether they were granted (as permitted by the policy) or rejected, are documented, and such documentation will be maintained and made available for review by ICANN on request. The registry′s monthly report to ICANN will contain per-registrar information on the granted add-deletes, as well as additional columns regarding the exemption requests.

The related report columns are (with column header names in parentheses):

1. number of AGP deletes (″domains-deleted-grace″)
2. number of exemption requests (″agp-exemption-requests″)
3. number of exemptions granted (″agp-exemptions-granted″)
4. number of names affected by granted exemption request (″agp-exempted-domains″)

5. Prevention of Domain Name Sniping (Grabbing)

Domain name sniping (also known as ″grabbing″) is another common abuse pattern; the name refers to the practice of trying to re-register potentially interesting domain names immediately after they are deleted (sometimes by accident, or because a registrant failed to renew the domain with his registrar in time).

Since .scot domains are (per registry policy) automatically renewed when they reach their expiration date, no explicit renewals by registrars are required to prevent a domain name from being deleted when they expire. Registrars need to explicitly delete domains in order to release them for re-registration. This substantially reduces opportunities for domain name sniping.

However, registrars may still send unintended domain deletions, i.e. due to clerical errors or miscommunication with the registrants. Even for these cases, measures against domain sniping are in place.Starting in 2002, registries have started to implement an ICANN proposal, the

so-called ″Redemption Grace Period″ (RGP, http://www.icann.org/en/registrars/redemption-proposal-14feb02.htm).

The proposal recommends introducing a 30-day period after a name's deletion during which the name is removed from the TLD zone (in order to give the registrant the chance to take notice of his name's deletion) but is still eligible for being restored by the previous registrar/registrant.

Supporting the RGP significantly reduces chances for domain grabbers to obtain inadvertently deleted domains, since a registrant gets 30 days to notice the mistake and restore the domain before it becomes available for re-registration.

The .scot Registry supports the Redemption Grace Period as proposed by ICANN and implements it in full compliance with RFC 3915 (″Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)″).

6. Prevention of Orphaned Glue Records

According to the definition found in the ″SSAC Comment on the Orphan Glue Records in the Draft Applicant Guidebook″ (http://www.icann.org/en/committees/security/sac048.pdf), a glue record becomes an ″orphan″ when the delegation point NS record (the ″parent NS record″) that references it is removed while retaining the glue record itself in the zone. Consequently, the glue record becomes ″orphaned″ since it no longer has a parent NS record. In such a situation, registrars and registrants usually lose administrative control over the record, and the record's attribution to a certain registrar may become unclear, which makes it a potential vector for abuse.

The glue record policy in effect for the .scot TLD avoids this situation entirely by disallowing orphan glue records altogether. This corresponds to policy #3 mentioned in section 4.3 (page 6) of the SSAC document mentioned above. The technical implementation within the Registry and its associated zone generation process ensures this by the following measures:

* As a general principle, glue records are only created if they are really necessary, i.e. only in the case where a name server (e.g. ″ns.example.scot″) is used for the delegation of a superdomain of its own name, e.g. ″example.scot″ in this example. If the same name server is used for e.g. ″example2.scot″, no glue record is created.

* A host object within the .scot TLD (e.g. ″ns.example.scot″) cannot exist without its parent domain (″example.scot″). Any attempt to create the host ″ns.example.scot″ will be rejected by the SRS if the domain ″example.scot″ does not already exist or is not sponsored by the registrar creating the host. Likewise, the domain ″example.scot″ cannot be deleted by the registrar if

subordinate hosts like ″ns.example.scot″ still exist. These subordinate hosts have to be deleted before the domain may be deleted; if such hosts are used in delegations for other .scot names, these delegations in turn have to be removed before the host may be deleted.

* If a domain name is put on hold (e.g. as a consequence of the Rapid Takedown Policy described above), this not only means that the delegation for the name itself is removed from the zone; it also means that any occurrences of NS records referencing a name server that is subordinate to the domain are also removed from other .scot domains, along with any accompanying glue records. The same of course holds true should the domain name have to be deleted entirely by the registry.

Consequently, no glue records can exist for a certain domain in the .scot zone after that domain is put on hold or deleted as part of abuse prevention or mitigation procedures.

It should be noted that this policy may lead to other domains (not directly involved in the abuse case) being affected by the takedown if they were delegated to a name server subordinate to the offending domain. Depending on their overall DNS architecture, such domains may become unreachable or less reachable after the delegation point is removed. While this could in theory be avoided by a less rigid orphan glue record policy, the overall benefit of adopting the strict policy described above is deemed higher than the potential damage to domains using an DNS infrastructure depending on an offending domain name.

7. Preventing Use of Trademarked, Reserved, Invalid, Illegal or Otherwise Unsuitable .scot Names

As laid out in the answer to Question 29 (Rights Protection Mechanisms), the .scot Registry takes extensive measures to protect the legal rights of others (such as trademark holders) with regard to .scot domain names. This includes

* conducting a Sunrise phase to allow trademark holders to secure names related to their trademarks prior to GA,

* accessing a Trademark Clearinghouse to validate trademarks presented by registrants,

* offering a Trademark Claims Service, at least during the first 60 days of general availability,

* taking precautions against phishing and pharming and

* committing to full compliance with established Dispute Resolution and Suspension Procedures, including the Uniform Rapid Suspension (URS), the Trademark Post-Delegation

Dispute Resolution Procedure (Trademark PDDRP), and the Uniform Domain Name Dispute Resolution Policy (URDP).

Please refer to the answer to Question 29 for more detailed information on these measures.

In addition to these specific rights protection measures, CORE Registration System provides the following general means to make sure that no .scot names are registered which are for other reasons deemed invalid, reserved, illegal, offensive or unsuitable.

7.1 Rule Engine

For the most part, this is achieved by the deployment of a complex rule engine that checks each registered name at the time of registration for compliance with a configurable set of rules. Among other things, these rules will include:

* a test to ensure that the domain name has the proper number of labels (which is two for a traditional registry that allows only second level domains to be registered),

* a test to ensure that no hyphens occur in position 3 and 4 of any of the domain's U-labels (to protect ″xn--″ and future ACE prefixes),--

* a test to disallow hyphens at the beginning or end of the name,

* a test to find ASCII characters which are neither a letter, nor a digit, nor a hyphen,

* a test to find invalid IDN characters, i.e. characters not contained in any of the support IDN character tables,

* a test to disallow reserved geopolitical names,

* a test to disallow registry reserved names,

* a test to disallow ICANN reserved names,

* a test to disallow otherwise reserved or unsuitable names.

Please refer to the answer to Question 44 (Internationalised Domain Names) for more information on the rules governing valid IDNs in the .scot TLD.

For the tests checking for reserved names, custom lists of labels can be conveniently maintained by the .scot Registry to define the disallowed names for each category. Additional categories can also be added as required for enforcing specific policies of the .scot TLD.

The rules are stored in database tables (rather than static configuration files), which means rules can be added, deleted or altered by authorised registry personnel without requiring a shutdown or restart of the .scot SRS.

7.2 Compliance with Specification 5 of the Registry Agreement

The rule engine is the central system component ensuring that the .scot Registry will operate the .scot TLD in full compliance with Specification 5 (″SCHEDULE OF RESERVED NAMES AT THE SECOND LEVEL IN GTLD REGISTRIES″) of the Registry Agreement. Unless the .scot Registry is otherwise authorised by ICANN and the Government Advisory Committee (GAC) in writing, the rule engine for .scot will be set up to prohibit the registration of the labels and label types listed in Specification 5 by registrars.

7.3 Pattern Matching and Fuzzy String Comparison

In addition to the pre-registration checks described above, the rule engine also supports testing registered domain names against a set of configurable string patterns, as well as for their similarity to a set of disallowed strings. The former is implemented by matching names against regular expressions, the latter by calculating the so-called ″Levenshtein distance″ between the registered name and a given disallowed string (which is a measure for their similarity). Prior to performing any of these checks, the registered name is subjected to a number of normalisations in order to maximise its comparability; this includes the mapping of IDN characters with accents to their ASCII counterparts where feasible, the removal of hyphens and the removal of digits.

If a name matches a regular expression, or if the calculated Levenshtein distance falls below a certain threshold, the name is still normally registered, however it is also internally flagged for review. Due to the fuzzy nature of the pattern and Levenshtein matching, a name flagged via these checks may not necessarily be invalid or illegal; this is why the flagged names need to be reviewed manually by the .scot support staff. Flagged names automatically create tickets within the support team′s issue system, which starts a workflow that ultimately decides whether the name is permissible (in which case the flag is removed) or invalid⁄illegal (in which case the name is deleted and the registrar gets notified).

7.4 Handling of IDNs

In the context of abuse prevention, the proper handling of Internationalised Domain Names (IDNs) becomes an important aspect.

If different IDN scripts were allowed to be mixed within one domain name, so-called homographs could be used to make users believe they are looking at a certain web site while it is actually a different one which name just has an identical or very similar visual representation. For example, since the Cyrillic letter ″Er″ (″p″ in Cyrillic script) in lower case has the same visual appearance as the Latin lower case letter ″p″, mixing Latin and Cyrillic scripts would allow the creation of a domain name like ″paypal.scot″, a homograph of the Latin-only name ″paypal.scot″ which, despite being a different word, looks exactly the same. Such a domain name could thus e.g. be used for spoofing or phishing attacks. The .scot Registry prevents such abuse by implementing an IDN policy that disallows the mixing of scripts; within each label of a registered .scot, only characters from a single script may be used.

Likewise, the Cyrillic-only second level domain ″pop.scot″ looks identical to its Latin-only counterpart ″pop.scot″. If only the rule described above (no mixing of scripts) would apply, these two names could coexist for different registrants, and could thus be abused to confuse users. However, the special way the .scot Registry handles such IDN variants while considering respective IDN tables and canonical forms of domain names, as described in detail in the answer to Question 44 (Support for Registering IDN Domains), prevents this situation; only one of these two domains may exist at the same time. In short, one singe table, Latin script, will be allowed.

The .scot Registry is aware that even within the same script (e.g., Latin), the use of diacritics may potentially cause similar confusion among users, e.g. if the ASCII-only name ″paypal.scot″ and a very similar one with diacritics (like ″páypàl.scot″) are coexisting as completely separate registrations. Hence, the .scot Registry has decided to treat such names as false variants and only allow their registration by the same registrant. Please see response to Question 44 below, and specially the IDN Table attached there, for further details.

8. Domain Data Access Control

One important point of attack that may lead to abuse of .scot domains and their associated data is the unauthorized or excessive access to data stored within the .scot repository. This applies to both read access (e.g. via public interfaces such as the port 43⁄port 80 Whois) and write access (such as registrar interfaces like EPP or the[8] web-based Control Panel). The measures taken in the .scot TLD to properly restrict access are laid out in the following sub-sections.

8.1 Prevention of Whois Data Mining

The port 43/port 80 Whois interfaces grant public access to domain, host and contact data. As such they are a potential target for data mining, i.e. the retrieval of large numbers of postal or e-mail addresses for e.g. the purpose of advertising.

As explained in detail in the answer to question 26 (Whois), the Whois implementation provided by the .scot Registration System prevents such data mining attempts, most importantly by:

* Access to all Whois interfaces is rate-limited (when accessed from IP addresses not whitelisted for unlimited access).

* Web interface users are required to pass a CAPTCHA before access is granted.

* Web interface users seeking access to extended Whois search capabilities are required to authenticate by entering login credentials (which are only issued to eligible parties).

* For improved spam protection, E-mail addresses may be displayed as images only in the web-based Whois.

* Contact disclosure flags as specified in RFC 5733, the Extensible Provisioning Protocol (EPP) Contact Mapping, are fully supported. This gives registrants enhanced control over the contact fields they want to disclose in the Whois. In this respect, the system is configurable and allows restricting the use of EPP contact disclosure settings via rules defined by specific registry policies or legal requirements.

8.2 Prevention of Unauthorized Data Modifications

Domain data within the .scot Registry is exclusively provisioned by registrars, i.e. registrants have no direct write access to their data within the repository; all their modifications have to be done via the registrar sponsoring the respective domain. In this constellation, registrants need to trust their registrar and will expect that the management of domain is conducted in a diligent and correct manner. This means that the registry's interfaces used by registrars need to be secured in order to only allow the sponsoring registrar of a domain (and nobody else) to modify domain data.

The EPP interface provided by the .scot Registration System does this by:

* requiring SSL/TLS on the transport layer,

* requiring a strong EPP password (minimum length, mandatory digits and non-alphanumerical characters),

* requiring changing the EPP password on a regular basis,

* requiring registrars to supply lists of IP addresses or subnets from which exclusive access will be granted,

* requiring registrars to use SSL client certificates known to and trusted by the registry, thus providing an additional means of authentication beyond the EPP password.

Likewise, the web-based Control Panel:

* requires SSL⁄TLS on the transport layer,

* requires registrars to log in with a user name and password (for which the same rules regarding minimum length, mandatory digits and non- alphanumerical characters apply),

* requires changing the password on a regular basis,

* requires registrars to supply lists of IP addresses or subnets from which exclusive access will be granted,

* requires registrars to install SSL client certificates known to and trusted by the registry in their web browsers, thus providing an additional means of authentication beyond the web password.

9. Whois Accuracy

Since .scot is operated as a so-called ″thick registry″, the .scot Whois displays information about the registrant, as well as the administrative, technical and billing contacts of every .scot domain. In cases of malicious or abusive activity involving a .scot domain, this Whois contact information usually is the first and most important source of information, e.g. for law enforcement authorities, to determine in a timely manner the people or organizations responsible for the domain. Consequently, it is deemed very important to maximize the accuracy of contact information stored in the registry repository.

The .scot Registry is therefore committed to taking diligent measures to promote Whois accuracy, including (but not limited to) the following:

* Contact data completeness policy: While RFC 5733, the Extensible Provisioning Protocol (EPP) Contact Mapping, merely requires contact data to contain a name, a city, a country code and an e-mail address for a syntactically complete EPP request, the .scot TLD policy for contact data mandates the specification of at least one address line (street), a voice phone number and a postal code in addition. This means that, in addition to the XML schema validation conducted

by the .scot SRS for every EPP request received from the registrar (which ensures the presence of all RFC-mandated contact data), the SRS also requires these essential fields to be present and will reject requests lacking them with a ″parameter value policy error″ message. The validation done by the SRS also goes beyond validating against the EPP XSDs with respect to field content. For instance, contact e-mail addresses are required to contain an ′@′ character and a valid domain name; this is not mandated by the XSDs specified in RFC 5733.

Contact data monitoring: On a regular basis, the registry will run automated plausibility audits on the contact data submitted by registrars. Using publicly available databases, contact address lines will e.g. be mapped to cities and zip codes, which are then compared to the ones provided by the registrant. Likewise, phone and fax numbers will be checked for plausibility.

* Domain data change notifications: [15] The .scot Registration System can be configured (on a per-registrar basis) to automatically notify certain contacts of a domain (e.g. both the registrant and the administrative contact in order to reach multiple people concerned with the domain) after every change made to the domain (i.e. alterations of associated contacts or name servers). When enabled, this feature allows unauthorized or unintended changes to domain and contact data to be detected immediately. This functionality will however need to be deployed after consultation with .scot registrars, since many registrars do not endorse direct communication between the registry and registrants, i.e. their customers.

* WDRP auditing: In 2003, ICANN adopted the so-called ″Whois Data Reminder Policy″ (WDRP, http://www.icann.org/en/registrars/wdrp.htm) which obliges ICANN-accredited registrars to send yearly Whois data reminder notices to registrants. These notices contain the Whois data currently on file for the respective domain, as well as instructions for the registrant about ways to correct the data if required. While the .scot Registry does not intend to replicate this reminder procedure on the registry level, it will establish an auditing process that monitors the WDRP activities of .scot registrars to make sure that WDRP responsibilities are honored.

9. Resourcing Plans

The CORE Registration System already supports the technical abuse prevention and mitigation measures above at the time of writing. No additional coding is required for this, which means that no special developing resources will be needed. Continuous audits and monitoring, as well as timely reactions to reports of malicious activity will be provided by the staff on duty at CORE Internet Council of Registrars.

For the initial setup, the following resources are allotted:

* Registry Policy Officer: finalising policies, creating documentation: 7 man days

* System Administrator: monitoring setup: 3 man days

* First Level Support: training: 1 man day per person

* Second Level Support: training: 1 man day per person

For the ongoing maintenance, the following resources are allotted:

* First Level Support: 10 man hours per month

* Second Level Support: 20 man hours per month

* System Administrator: 3 man hours per month

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by CORE in the past over the course of 12 months.

2. Compliance Mechanisms. General Availability

As explained in questions 18 and 20, once in Ongoing (live) Registration mode, the .scot Registry will perform ex-post validation based on Whois data and use of the domain name, both against the Registrations Policies and the Intended Use Statement provided by the registrant at registration time (or updated afterwards).

2.1 Ex-officio random checks

Checks will be performed by compliance agents both based on complaints and ex-officio, through statistically targeted random checks. The .scot Registry will start with 50 such random cases per day, and will adapt the practices according to the experience gained (it is expected that the number will decrease over time, as reputation and enforcement will make compliance easier over time).

Checks will be carried out both on compliance with the .scot TLD policy and, at the same time, on registrant data accuracy.

In case the compliance agents discover any problem, they will forward the issue to the Compliance Officers, and the registrant will be contacted to clarify/correct the situation. If not solved in due time (15 or 30 days, according to the specific cases), the name may be put on registry hold.

2.2 Complaints, Rights Protection

Similarly, in case of a third party complaint for infringement of rights of others, the Compliance Officers will request the complainant to compile a specific form including such information as :

* identification of complainant,

* identification of infringed right,

* declaration of good faith belief that the domain name is used to violate said right,

* indemnification of the Registry in case of action based on false, inaccurate or otherwise non-applicable claims,

* acceptance of jurisdiction of the courts of Edinburgh and Registrant's domicile, in case the name is blocked and the registrant wants to sue the complainant for damages.

Then the registrant will be contacted. In case the registrant provides within the following 15 business days a counter-statement with some specific content (identification; signed declaration of non-infringement of rights, with explanation of reasons) the domain name will not be blocked, and the complainant shall use the Uniform Rapid Suspension procedure, the UDRP, the .scot TLD Charter Compliance Dispute Resolution Procedure (CCDRP) or file a lawsuit in a competent court. In case the registrant fails to provide all the elements (which will often be the case in blatant violations) the domain name could be put on registry hold.

Against these decisions (not just for Rights Protections, but also in cases of Compliance decisions for Eligibility or use breaches and malicious conduct) the parties may appeal to an independent Mediation and Arbitration Authority according to the .scot TLD CCDRP.