Security Disclosure Policy

The Expert Assessment Solutions (**EAS**) greatly appreciates investigative work into security vulnerabilities that well-intentioned, ethical security researchers carry out. We are committed to thoroughly investigating and resolving security issues in our platforms and services in collaboration with the security community. This document aims to define how the EAS can work with the security research community to improve our online security.

Scope

Vulnerabilities in EAS products and services are only within the scope of the Bug Bounty Scheme when they meet the following conditions:

- They have not been previously reported or have not already been discovered by our own internal procedures.
- It can be demonstrated that there would be a real impact to the BBC, its users, or its customers should the vulnerability reported be exploited by a malicious actor. The existence of a vulnerability does not necessarily demonstrate that such a potential impact exists theoretical impacts will not be considered as within the scope of the scheme.

The following security issues are currently not in scope (please don't report them):

- Volumetric/Denial of Service vulnerabilities (i.e., simply overwhelming our service with a high volume of requests);
- Reports indicating that our services do not fully align with "best practice" (e.g., missing security headers or suboptimal email-related configurations such as SPF, DMARC, etc.);
- Issues surrounding the verification of email addresses used to create user accounts;
- Self XSS (i.e., where a user would need to be tricked into pasting code into their web browser);
- CSRF where the resulting impact is minimal;
- CRLF attacks where the effect is minimal;
- Host header injection where the resulting impact is minimal;
- Reports of improper session management/session fixation vulnerabilities.

Bug Bounty

Unfortunately, due to the EAS's funding structure, it is not currently possible for us to offer a paid bug bounty program. We would, however, like to provide a token of our appreciation to security researchers who take the time and effort to investigate and

report security vulnerabilities to us according to this policy. Reporters of qualifying vulnerabilities will be offered a unique EAS reward.

Reporting a vulnerability

If you have discovered an issue which you believe is an in-scope security vulnerability (please see section 2 above for more detail on scope), please email info@aCodec.com or info@lenavipro.com, including:

- The website or page in which the vulnerability exists.
- A brief description of the type of vulnerability. *Please avoid including any details which would allow reproduction of the issue at this stage.* The part will be requested subsequently over encrypted communications.

In accordance with industry convention, we ask that reporters provide benign (i.e., non-destructive) proof of exploitation wherever possible. This helps ensure that the report can be triaged quickly and accurately whilst also reducing the likelihood of duplicate reports and/or malicious exploitation for some vulnerability classes (e.g., sub-domain takeovers). Please ensure that you do not send your proof of exploit in the initial, plaintext email if the vulnerability is still exploitable. Please also ensure that all evidence of exploits are by our guidance (below). If you are in any doubt, please email info@aCodec.com for advice.

Please read this document thoroughly before reporting any vulnerabilities to ensure that you understand the policy and can act in compliance with it.

What to expect

In response to your initial email to info@acodec.com, you will receive an acknowledgment reply email from the EAS Security Team (**EAS ST**). This is usually within 24 hours of your report being received. The acknowledgment email will include a ticket reference number which you can quote in any further communications with our Security Team. In addition, attached to the acknowledgment email will be a Pretty Good Privacy **PGP** key that you can use to encrypt future communications containing sensitive information.

Following the initial contact, our **EAS ST** Security Team will triage the reported vulnerability. It will respond to you as soon as possible to confirm whether further information is required and / or whether the vulnerability qualifies as per the above scope or is a duplicate report. From this point, necessary remediation work will be assigned to the appropriate EAS teams and / or supplier(s). Based on the severity of impact and complexity of exploitation, priority for bug fixes and/or mitigations will be assigned. Vulnerability reports may take some time to triage and/or remediate, and

you're welcome to enquire on the status of the process but please limit this to no more than once every 14 days. This helps our **EAS ST** team focus on the reports as much as possible.

EAS ST Security Team will notify you when the reported vulnerability is resolved (or remediation work is scheduled) and ask you to confirm that the solution adequately covers the vulnerability. In addition, we will offer you the opportunity to feedback to us on the process and relationship as well as the vulnerability resolution. This information will be used in strict confidence in order to help us improve the way in which we handle reports and/or develop services and resolve vulnerabilities. We will also offer to include reporters of qualifying vulnerabilities on our acknowledgments page, and we'll ask for the details you wish to be included.

Guidance

Security researchers must not:

- Access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities (such as an enumeration or direct object reference vulnerability);
- Violate the privacy of aCodec users, staff, contractors, systems, etc. For example, by sharing, redistributing and/or not properly securing data retrieved from our systems or services;
- Communicate any vulnerabilities or associated details via methods not described in this policy or with anyone other than your dedicated **EAS ST** security team contact;
- Modify data in our systems/services which is not your own;
- Disrupt our service(s) and / or systems; or
- Disclose any vulnerabilities in EAS systems/services to 3rd parties/the public before the EAS confirms that those vulnerabilities have been mitigated or rectified. This does not prevent notification of a vulnerability to 3rd parties to whom the vulnerability is directly relevant, for example, where the vulnerability being reported is in a software library or framework – but details of the specific vulnerability of the EAS must not be referenced in such reports. If you are unsure about the status of a 3rd party to whom you wish to send a notification, please email info@acodec.com for clarification.

We request that any and all data retrieved during research is securely deleted as soon as it is no longer required and, at most, one month after the vulnerability is resolved, whichever occurs soonest.

If you are unsure at any stage whether the actions you are thinking of taking are acceptable, please get in touch with our security team for guidance (please do not include any sensitive information in the initial communications): info@acodec.com.

Legalities

This policy is designed to be compatible with standard good practices among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law or cause the **EAS** to be in breach of any of its legal obligations, including but not limited to:

- The Computer Misuse Act (1990)
- The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018
- The Copyright, Designs, and Patents Act (1988)

The EAS will not seek prosecution of any security researcher who reports any security vulnerability on an in-scope EAS service in good faith and following this policy.

Feedback

If you wish to provide feedback or suggestions on this policy, please contact our **EAS ST** security team: info@acodec.com.