Responsible Disclosure Policy

KaR-Tel LLP ("Beeline" TM) cares about the security of the data, services and facilities we offer our customers. If you believe, you have discovered potential vulnerability in our services; we would appreciate your help in disclosing this vulnerability for us.
This document (hereafter the "Policy") provides information on how to report vulnerabilities and thanks the security researchers who have reported vulnerabilities in the past.

How we approach the safety reports

- Beeline will not take legal action against users for disclosing vulnerabilities where the following rules have been complied with in the disclosure. Beeline retains all its legal rights in the event of any failure to comply with applicable laws and regulations
- We always respond to reliable vulnerability reports as quickly as possible - usually within 2 business days
- Researchers who provide us with a valid report under this Policy confirm their consent to have their data placed on this page to express their appreciation and gratitude from Beeline once the vulnerabilities have been accepted, confirmed and corrected by our security team. Please let us know further if you want us to include a link to your social media account or alternatively, you do not want your details to be posted on this page
- Public disclosure of any identified or suspected vulnerability without the express written consent of Beeline will be considered inconsistent with this Policy

Reporting

If you think you have found a security problem with our service or service, send it to us at security@beeline.kz along with your contact details and include the following in your report

- Description of the vulnerability and its location together with screenshots
- Description of the steps required to reproduce the vulnerability

Beeline services are located on beeline.kz subdomains or on separate domains, please ensure that the domain belongs to Beeline.
Do not put Beeline customers' data at risk and do not compromise the performance of our services. Beeline reserves the right to take legal action and/or report to the relevant authorities the person who conducts any tests or investigations that are prohibitive, inconsistent with the law of the Republic of Kazakhstan, or inconsistent with this Policy.

Third-party services

Some beeline.kz subdomains are operated through third-party services. If you find a vulnerability in one of these subdomains, you can report it directly to the relevant company, using the contacts listed on subdomain. Please check that the Beeline subdomain belongs to Beeline before looking for a vulnerability.

Regulations for finding the vulnerabilities

- Proceed with extreme care and attention
- When carrying out a safety study, use only those methods or techniques that are not against the

law and that are necessary to identify or demonstrate weaknesses

- Do not use scanners or automated tools to find vulnerabilities
- Do not install any backdoors - not even to demonstrate the vulnerability of the service
- Posting, transmitting, downloading, linking, sending or storing any malicious software
- For security research, only work with accounts that are registered to you
- Do not modify our data or the data of our users, and do not access other people's accounts
- Do not view, modify, save, or store, not transmit or otherwise gain access to any data, received accidentally during your research, and immediately clear any local information after reporting a vulnerability to Beeline
- Act in good faith to avoid confidentiality breaches, data destruction and interruption or degradation of our services (including denial of service). Do not take any action that could compromise the reliability or integrity of our services and data
- Comply with applicable laws

We will not negotiate in response to coercion or threats (for example, we will not offer a monetary reward and will not negotiate a payment amount under threat of withholding vulnerability or threat of disclosure of vulnerability or any disclosed data to the public).

The following categories of vulnerabilities and attacks are considered to be outside the scope of the Policy (unless a proven high impact is demonstrated):

- Vulnerabilities requiring the use of social engineering
- Brutforce
- Execution or attempted execution of any “DoS/DDoS” attack
- Vulnerabilities affecting only legacy user agents or versions of applications
- Testing in a way that may result in the sending of unwanted or Unauthorized junk mail, spam, pyramid schemes or other forms of duplicate or unwanted messages
- Testing in a way that may impair the operation of any Beeline services; or testing third-party applications, websites or services that integrate with Beeline services
- No “Safe” marking, no “HTTP Only” flag for non-confidential cookies
- Vulnerabilities that require a potential victim to install non-standard Software or other actions to become vulnerable to attack.
- UI/UX errors and spelling mistakes
- Spam
- Disclosure of known publicly accessible files or directories (e.g. robots.txt)
- Clickjacking and vulnerabilities that can only be exploited by clickjacking
- CSRF in forms accessible to anonymous users (e.g. contact form).
- Cross-site request forgery (CSRF) with low security affects (Logout CSRF, etc.)
- Auto-complete or save your password in an app or web browser
- SSL attacks such as BEAST, BREACH, Renegotiation attack
- SSL Forward secrecy not enabled
- SSL insecure cipher suites
- The Anti-MIME-Sniffing header X- Content-Type-Options
- No HTTP security headers
- Self XSS

Special thanks to all those who helped Beeline:

2022:

- Gaurang Maheta

2019:

- Batyrzhan Tyuteyev

Политика ответственного раскрытия информации

ТОО «КаР-Тел» (далее – Beeline) заботится о безопасности данных, услуг и сервисов, которые мы предлагаем нашим клиентам. Если вы считаете, что обнаружили потенциальную уязвимость в наших сервисах, мы оценим вашу помощь в раскрытии этой уязвимости для нас.
Данный документ (далее – Политика) содержит информацию о том, как сообщить об уязвимости, и благодарит исследователей безопасности, которые сообщали об уязвимостях в прошлом.

Как мы подходим к отчетам о безопасности

- Beeline не будет предпринимать юридических действий против пользователей за раскрытие уязвимостей, в случае если при раскрытии были соблюдены указанные ниже правила. Beeline сохраняет все свои законные права в случае любого несоблюдения применимых законов и правил
- На достоверные отчеты об уязвимостях всегда отвечаем как можно более быстрый ответ – обычно в течение 2 рабочих дней
- Исследователи, которые предоставят нам валидный отчет в рамках этой Политики, подтверждают свое согласие на размещение своих данных на этой странице для выражения признательности и благодарности от Beeline, как только уязвимости будут приняты, подтверждены и исправлены нашей командой безопасности. Пожалуйста, сообщите нам дополнительно, если вы хотите, чтобы мы включили ссылку на вашу учетную запись в социальной сети или, напротив, не хотите, чтобы ваши данные были размещены на этой странице
- Публичное раскрытие информации о любой выявленной или предполагаемой уязвимости без явного письменного согласия Beeline будет считаться несоответствующим настоящей Политике

Репортинг

Если вы считаете, что обнаружили проблему безопасности в нашем сервисе или услуге, отправьте ее нам по адресу security@beeline.kz вместе со своими контактными данными и включите в отчет следующее:

- Описание уязвимости и ее расположение вместе со скриншотами экрана
- Описание шагов, необходимых для воспроизведения уязвимости

Сервисы Beeline расположены на поддоменах beeline.kz либо на отдельных доменах, пожалуйста, убедитесь, что домен принадлежит Beeline.
Не подвергайте риску данные клиентов Beeline, не снижайте производительность наших сервисов.
Beeline оставляет за собой право возбудить судебный иск и/или сообщить в соответствующие органы о лице, которое проводит какие-либо тесты или расследования, которые являются запретительными или не соответствуют закону Республики Казахстан или не соответствуют настоящей Политике.

Услуги третьих лиц

Некоторые поддомены beeline.kz работают через сторонние сервисы. Если вы обнаружите уязвимость на одном из таких поддоменов, вы можете сообщить об этом непосредственно в соответствующую компанию, по контактам, указанным на поддомене. Пожалуйста, проверьте принадлежность поддомента Beeline перед тем, как искать уязвимость.

Правила поиска уязвимостей

- Действуйте с особой осторожностью и вниманием
- При исследовании на безопасность используйте только те методы или приемы, которые не противоречат закону и необходимы для выявления или демонстрации слабых мест
- Не используйте сканеры или автоматизированные инструменты для поиска уязвимостей
- Не устанавливайте никаких бэкдоров – даже для демонстрации уязвимости сервиса
- Размещение, передача, загрузка, ссылка, отправка или хранение любого вредоносного программного обеспечения
- В целях исследования безопасности работайте только с учетными записями, зарегистрированными на вас
- Не изменяйте наши данные или данные наших пользователей, не получайте доступ к чужим учетным записям. Не просматривайте, не изменяйте, не сохраняйте, не храните, не передавайте и не получайте иным образом доступ к любым данным, полученным случайно во время вашего исследования, и немедленно очищайте любую локальную информацию после сообщения об уязвимости в Beeline
- Действуйте добросовестно, чтобы избежать нарушения конфиденциальности, уничтожения данных, а также прерывания или ухудшения качества наших услуг

(включая отказ в обслуживании). Не выполняйте никаких действий, которые могут нанести ущерб надежности или целостности наших услуг и данных
- Соблюдайте все применимые законы

Мы не будем вести переговоры в ответ на принуждение или угрозы (например, мы не предлагаем денежное вознаграждение и не будем вести переговоры о сумме выплаты под угрозой удержания уязвимости или угрозы раскрытия уязвимости или любого раскрытых данных для общественности).

Следующие категории уязвимостей и атак считаются выходящими за рамки Политики (если не будет продемонстрировано доказанное высокое воздействие):

- Уязвимости, требующие использования социальной инженерии
- Брутфорс
- Выполнение или попытка выполнения любой атаки типа «DoS/DDoS»
- Уязвимости, затрагивающие только устаревшие пользовательские агенты или версии приложений
- Тестирование способом, который может привести к отправке нежелательной или несанкционированной нежелательной почты, спама, финансовых пирамид или других форм дублирующих или нежелательных сообщений
- Тестирование способом, который может ухудшить работу любых сервисов Beeline; или тестирование сторонних приложений, веб-сайтов или служб, которые интегрируются с сервисами Beeline
- Отсутствие пометки "Безопасно", отсутствие флага "HTTP Only" для неконфиденциальных cookie
- Уязвимости, требующие от потенциальной жертвы установки нестандартного программного обеспечения или иных действий, чтобы стать уязвимыми для атаки.
- Ошибки UI/UX и орфографические ошибки
- Спам
- Раскрытие известных общедоступных файлов или каталогов (например, robots.txt)
- Кликджекинг и уязвимости, которые можно использовать только с помощью кликджекинга
- CSRF в формах, доступных анонимным пользователям (например, контактная форма).
- Межсайтовая подделка запросов (CSRF) с низким воздействием на безопасность (Logout CSRF и т.д.)
- Наличие функции автозаполнения или сохранения пароля в приложении или веббраузере
- SSL-атаки, такие как BEAST, BREACH, Renegotiation атака
- Не включена SSL Forward secrecy
- Наборы небезопасных шифров SSL
- Заголовок Anti-MIME-Sniffing X-Content-Type-Options (The Anti-MIME-Sniffing header XContent-Type-Options)
- Отсутствие HTTP security headers

- Self XSS

Отдельное спасибо всем тем, кто помог Beeline:

2022:

- Gaurang Maheta

2019:

- Батыржан Тютеев