NORTONLIFELOCK GLOBAL PRIVACY STATEMENT

Introduction
When it comes to your personal data, NortonLifeLock and its subsidiaries (collectively referred to as “NortonLifeLock”, “Norton”, “LifeLock”, “we”, or “us”), as well as our employees, contractors, and service providers, are committed to providing you with transparency. We process personal data in accordance with applicable legislation.

We do not, and will not without consent, sell, lease, or rent your information to third parties for monetary or other valuable consideration.

This Privacy Statement (“Statement”) applies to the NortonLifeLock websites, services, and products (our “Services”) that link to or reference this Statement. In this Statement, we describe how we collect, process, and share personal data, and the choices available to you regarding collection and use of your personal data.

Additional information on our personal data practices may be provided in product descriptions, contractual terms, supplemental privacy statements, or notices provided prior to or at the time we collect your data. Please see www.nortonlifelock.com/privacy for more details about what personal data we collect and how we process that personal data.

If you are in the European Economic Area, and unless stipulated otherwise contractually, the Controller of your personal data is:

NortonLifeLock Ireland Limited
Ballycoolin Business Park
Blanchardstown
Dublin 15
Ireland D15E867

Categories of Personal Data We Collect:
The categories of personal data that we collect, and the general purposes of collection, include:

- **User Data.** This data is necessary to establish your account and method/means of payment, ship and provide your services, and track and maintain our relationship with you. It includes:
  - Name, mailing address, email address, phone number, and user credentials (login name and password);
  - Shipping and billing data, including credit card and payment data;
  - Your social security number and/or state/government identifier, driver’s license number or other government-issued identifier, date of birth, age, gender, and other personal details about you as necessary to verify your identity and to provide identity theft protection services;
  - Bank transaction and other alert data depending on the product and features you have selected; and
  - Your transaction and support history with us.

- **Administrative Data.** This includes data we receive from you and from third parties that is necessary to facilitate installation of our products and may include device and system information, product license information, and/or
usage and preference information, including how you would like us to communicate with you. This data helps us better understand and better serve your interests, expectations, needs, and requirements.

- **Security Data.** This data may include financial transactions, location data, and data that is collected for cyber threat intelligence, as needed to provide cyber safety and identity threat protection Services.

- **Diagnostic Information.** This data may include application crash reports and information you provide to us for obtaining customer service, as necessary, to troubleshoot any malfunctioning Services. For example, when you call or exchange email, chat, or mail with us, we may retain and review call and chat recordings and/or the contents of the messages as required/permitted by law and our recording and information management policies.

- **Third-Party Data.** This information includes data we may obtain about you from a third party, or data provided about you from a third party through the use of our Services, including threat intelligence data used to analyze threats and protect you, us, and our other customers against cyber threats. Third-party data may include the email and IP address of the sender of malicious malware.

**The Purpose of Processing Your Personal Data**

We collect and process your personal data for the following reasons:

**For the purpose of fulfilling our contract** with you at your request, in order to:

- Create and manage your account;
- Authenticate your identity prior to enrolling in our Services;
- Verify your identity and entitlement to Services, when you contact us or access our Services;
- Process your purchase transactions;
- Update you on the status of your orders;
- Allow you to register the Services you purchase;
- Manage your subscriptions; and
- Provide you with technical and customer support.

**For specific purposes based on your consent,** in order to:

- Subscribe you to newsletters and send you product updates or technical alerts;
- Send you marketing communications and information on new Services;
- Communicate with you about, and manage, your participation in contests, offers, or promotions;
- Solicit your opinion or feedback and/or provide opportunities for you to test Services;
- Enable you to refer a friend who may be interested in our offerings, as permitted by law;
- As applicable, to enable non-essential cookies or similar technologies;
- Process sensitive or special category personal data in accordance with applicable law; and
- As applicable, to provide you with interest-based ads about NortonLifeLock on sites other than our own.

**For the purpose of fulfilling our legal obligations,** we may be obligated to, for instance, keep and process records for tax purposes, accounting, other obligations such as court or other legal orders, and other necessary disclosures.
For the purpose of promoting and operating our business and advancing our legitimate interests, such as the effective delivery of our Services, and communications to you as well as to our other customers and partners, in order to:

- Provide you with information and Services that you request;
- Enable participation in interactive features of our Services, and notify you about changes to our terms or this Privacy Statement;
- Communicate commercial promotions and provide quotes for our Services;
- Promote and administer co-branded offers with trusted partners;
- Confirm sales conversions and conduct lead generation activities;
- Better administer and understand the usability, performance, and effectiveness of our Services, including troubleshooting, data analytics, testing, research, and statistical analysis;
- Improve our Services (including developing new Services) and customize and present content in the most relevant and effective manner for you and for your device, including suggestions and recommendations about things that may be of interest to you;
- *Enhance the security of our own networks and information systems;
- *Develop cyber-threat intelligence resources; and
- *Otherwise keep our Services, business, and users safe and secure, and comply with applicable laws and regulations to protect or exercise our legal rights and defend against legal claims.

*For Network and Information Security Purposes and Cyber-Threat Intelligence:

Our legitimate interests include developing threat intelligence resources aimed at maintaining and improving the ability of our information networks and systems to resist unlawful or malicious actions and other harmful events, such as cybercriminal activities, and attempts at identity theft or fraud (“cyber and identity threats”).

The personal data we process for network and information security purposes includes, without limitation, network traffic data related to cyber and identity threats such as:

- Sender email addresses (e.g., of sources of SPAM such as phishing scams);
- Recipient email addresses (e.g., of victims of targeted email attacks);
- Reply-to email addresses (e.g., as configured by cybercriminals sending malicious email);
- Filenames and execution paths (e.g., of malicious or otherwise harmful executable files attached to emails);
- URLs and associated page titles (e.g., of web pages broadcasting or hosting malicious or otherwise harmful content);
- IP addresses (e.g., of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching, or other storage of cyber and identity threats such as malicious or otherwise harmful content); and/or
- Browser information (e.g., user agent string and session within cookies).

Depending on the context in which such data is collected, the data may contain personal data concerning you or third parties. However, in such cases, we will process the data only to the extent strictly necessary and proportionate to the purposes of detecting, blocking, reporting (by removing any personally identifiable elements), and mitigating the
cyber or identity threats of concern or those of other users relying on our Services to protect their networks, systems, and identities. When processing personal data in this context, we will only identify specific data subjects if and to the extent necessary for the remediation of the cyber or identity threats concerned, or as required by law.

Please be aware that if it is determined that personal data concerning you is processed by NortonLifeLock because it is necessary for the detection, blocking, or mitigation of convicted cyber or identity threats, then objection, rectification, or erasure requests may be rejected in accordance with applicable law.

How We Collect Your Personal Data
We collect personal data about you from the following sources:

Data you provide:
- When you interact directly with us, we may collect personal data that you provide to us (e.g., account and payment information).

Data we collect automatically:
- When you visit and use our websites and Services, we may automatically collect data about your interaction with our websites and Services.

Data we collect about you from third parties:
- Credit reporting agencies and financial institutions (used for purposes such as identity theft protection Services);
- Marketing and joint-marketing partners (used for purposes such as to offer Services and/or joint Service bundles to prospective members);
- Public sources such as the dark web to alert you to potential misuse of your data;
- Private sources for purposes of providing customers with alerts related to financial transactions, property title, social media abuse, and other types of alerts within our products; and
- We may collect personal data from you about other people, such as personal data about friends and family through customer or employee referrals, or data about family members you include on your account.

When and Why We Share Your Personal Data
We are committed to maintaining your trust, and we want you to understand when and with whom we may share the information we collect. We do not, and will not without consent, sell, lease, or rent your information to third parties for monetary or other valuable consideration.

We permit third parties to process information necessary for our Services, and we may disclose the personal information we process to third parties for business purposes. The third parties we work with are contractually required to comply with adequate privacy, confidentiality, and security requirements.

With our Partners
We may provide your user data, administrative data, security data, and third-party data to our partners for the purpose of allowing them to conduct NortonLifeLock business. Our partners may use your personal data to communicate with you and others about NortonLifeLock Services either alone or jointly with partner products and services. We may provide your personal data to partners to confirm your eligibility for joint or co-branded offers or to communicate and administer such offers (e.g., report sales conversions, verify eligibility, assess effectiveness of joint offer, etc.). Our partners are not allowed to use personal data that they receive from us for any purpose except for communicating, evaluating, improving, and
administering the offer in question (NortonLifeLock branded, co-branded, or joint offer). This will not affect the partner’s ability to use personal data that it may already have obtained from you or other sources. If you do not wish to receive promotional emails from our partners, you can unsubscribe directly using the unsubscribe link or tool provided in the partner’s email or other communication to you.

**With Service Providers Processing Data on Our Behalf**

We may use contractors and service providers to process the personal data we collect for the purposes described in this Statement, the relevant Product and Service Privacy Statements, and for business purposes such as financial auditing, data storage and security, troubleshooting and debugging, improving and operationalizing threat intelligence and counter-threat measures, and for marketing and promoting our Services.

We contractually require service providers to keep data confidential, and we do not allow our service providers to disclose your personal data to others without our authorization, or to sell it or use it for purposes unrelated to the services they provide (e.g., their own marketing purposes). However, if you have a separate and/or independent relationship with these service providers, their privacy statements will apply to such relationships. Such service providers may include benefit brokers, your employer (for products and services offered as an employee benefit), contact centers, payment card processors, and marketing, survey, or analytics suppliers.

**With Public Authorities and Legal Proceedings**

In certain instances, it may be necessary for us to disclose any of the personal data we collect to comply with a legal obligation, at the request of public authorities, or as otherwise required by applicable law. No personal data will be disclosed except in response to:

- A subpoena, warrant, or other legal process issued by a court or other public authority of competent jurisdiction;
- Discovery requests or demands as part of a civil lawsuit or similar legal process;
- Where disclosure is necessary for us to enforce our legal rights pursuant to applicable law;
- A request with the purpose of identifying and/or preventing credit card fraud or identity theft; or
- Where disclosure of personal data is necessary to prevent or lessen a serious and imminent threat of bodily or other significant harm to the data subject or other individuals potentially concerned.

**For Restoration Services**

We may disclose your user data, security data, diagnostic information, and third-party data to financial institutions, financial services companies, and other third parties at your direction to provide restoration services and other Services to you.

**With Third-Party Service Providers**

If you access third-party services through our Services, these third-party services may be able to collect user data, security data, diagnostic information, and third-party data about you in accordance with their own privacy policies.

**With Our Corporate Affiliates**

We may share all of the information we collect with our corporate affiliates.

**For Business Transfers**

We may share all of the information we collect in connection with a substantial corporate transaction, such as the sale of a website, a merger, acquisition, consolidation, asset sale, or initial public offering, or in the unlikely event of bankruptcy.
Retention and Deletion of Your Personal Data
We will keep your personal data on our systems as long as necessary to provide you with our Services, or for as long as we have another legitimate business purpose to do so, but not longer than permitted or required by law. When we no longer have an ongoing legitimate business reason to keep your personal data, your personal data will either be securely disposed of, or de-identified through an appropriate anonymization means, such as aggregation, truncation, or one-way hashing so it is no longer identifiable as your personal data.

Cross-Border Transfers of Personal Data Among NortonLifeLock Entities and to Third-Party Vendors
We are a global company and process personal data in many countries. As part of our business, your personal data may be transferred to NortonLifeLock and/or its subsidiaries and affiliates in the United States, and to subsidiaries and third-party vendors of NortonLifeLock located worldwide. All transfers will occur in compliance with the applicable data transfer requirements laws and regulations.

If your personal data originates from the European Economic Area and is transferred to NortonLifeLock subsidiaries, affiliates, or third-party vendors engaged by NortonLifeLock to process such personal data on our behalf who are located in countries that are not recognized by the European Commission as offering an adequate level of personal data protection, such transfers are covered by alternate appropriate safeguards, specifically Standard Contractual Clauses adopted by the European Commission.

If we are involved in a reorganization, merger, acquisition, or sale of our assets, your personal data may be transferred as part of that transaction.

How We Protect Your Personal Data
Securing personal data is an important aspect of protecting privacy. We take reasonable and appropriate physical, technical, and organizational security measures in accordance with applicable laws to protect your personal data against the risk of accidental loss, compromise, or any form of unauthorized access, disclosure, or processing. The relevant security controls are communicated throughout NortonLifeLock to support the secure development of Services and maintain a secure operating environment. Our security approach includes:

Physical Safeguards
We lock doors and file cabinets, control access to our facilities, implement a clean desk policy, and apply secure destruction to media containing personal data.

Technical Safeguards
We implement and use reasonably available state-of-the-art network and information security standards, protocols, and technologies, including encryption, intrusion detection, and data loss prevention, and we monitor our systems and data centers to comply with our security policies.

Organizational Safeguards
We conduct regular company-wide as well as role-specific training and awareness programs on security and privacy.

If you have any questions about the security of your personal data or the security of the site, or wish to report a potential security issue, please contact security@nortonlifelock.com. When reporting a potential security issue, please describe the matter in as much detail as possible and include any information that might be helpful. If you are having problems accessing your account, please contact our Member Support Center.
Your Privacy Rights

You can view and update your personal data through your Norton Account or LifeLock Portal. There are a variety of data protection laws around the globe that provide privacy rights to you as our customer. Subject to applicable laws, you may have the following rights:

- **Delete**: Right to delete or erasure (“right to be forgotten”) of personal data we have collected about you;
- **Access**: Right to access the personal data we have collected about you, as well as other information about our data processing practices;
- **Rectify**: Right to rectify, correct, update, or complement inaccurate or incomplete personal data we have about you;
- **Restrict**: Right to restrict the way we process your personal data;
- **Withdraw Consent**: Right to withdraw your consent to process your personal data;
- **Object**: Right to object to our processing of your personal data based on legitimate interest;
- **Portability of Personal Data**: Right to obtain a portable copy of your personal data; and
- **Lodge a Complaint**: Right to lodge a complaint with a supervisory authority if you are not satisfied with the way we have handled your personal data, or any privacy request, or other request that you have raised with us.

To exercise any of your rights, or to raise any other questions, concerns, or complaints about our privacy practices, or about our use of your personal data and its privacy, or if you are not a customer of ours and want to know what personal data we have about you, please contact us as explained below (“Contact Us”).

Once we receive your request, we will verify your identity and your authorization to take the actions requested, authenticating your identity at a level appropriate to the requested action. We require you to re-authenticate before we will disclose or delete data. You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent to exercise your rights and choices on your behalf, please contact NortonLifeLock Support.

In some instances, we are unable to delete or erase your personal data upon request as a result of an ongoing legal obligation such as a legal hold or court order. Depending on your location, there may be other restrictions or exemptions to full deletion or erasure of your personal data.

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features available on a Service may change or no longer be available to you where the processing of certain data is essential to the use of the Service or feature.

Contact Us

**Americas**

**NortonLifeLock Inc. – Privacy**
60 East Rio Salado Parkway, Suite 1000
Tempe, AZ 85281
Email: nll_privacy@nortonlifelock.com

**Member Services**: 1-800-543-3562
Europe – Middle East – Africa

NortonLifeLock Ireland Limited – Global Privacy Office
Ballycoolin Business Park
Blanchardstown
Dublin 15
Ireland D15E867
Email: nll_privacy@nortonlifelock.com

Independent EU GDPR Data Protection Officer
Pembroke Privacy Ltd
4 Upper Pembroke Street
Dublin 2
Ireland DO2VN24
Email: DPO@nortonlifelock.com

Referrals
When you choose to provide us with personal data about third parties, we will only use this data for the specific stated reason that you provided it. It is your responsibility to abide by applicable privacy and data security laws when you disclose third parties’ personal data to us, including informing third parties that you are providing their personal data to us and how it will be transferred, used, or processed, and securing the appropriate legal permissions and safeguards. If you choose to provide us with a third party’s personal data, you represent that you have the third party’s permission to do so. Examples include forwarding references or sending job referrals. You also acknowledge that when we interact with such third-party individuals whose personal data you share with us, it is our duty to inform them that we obtained their personal data from you. Where applicable, third parties may unsubscribe from any future communication following the link provided in the initial message. If you believe that one of your contacts has provided us with your personal data and you would like to request that it be removed from our database, please contact us.

Marketing and Community Networking
You may receive marketing messages and materials from us or our affiliates.

You have choices on what communications you wish to receive from us. If you do not want to continue receiving any marketing materials from us, you have the following options:

- Click on the unsubscribe function in the communications you receive from us;
- [Unsubscribe from Norton Marketing Offers](#);
- Manage your communication preferences in your Norton Account or LifeLock Portal;
- Contact our Member Services Department at 1-800-543-3562; or
- Contact our Member Services Department by regular mail at Attn.: Member Services, 60 East Rio Salado Parkway, Suite 1000, Tempe, AZ 85281.

If you choose not to receive marketing communications from us, we will honor your request.

However, we will continue to communicate with you as needed to provide the Services you are entitled to, to respond to your inquiries, or to otherwise relay transactional product or service-related messages.
Please also be aware that you may still receive information about our Services through other parties using their own mailing lists. For instance, marketing materials for our Services may also be contained in messages you receive from third parties, such as your employer if they offer our Services as part of their employee benefits.

Interest-Based Ads

We may provide your data, including the data about your interests in our Services, to third parties for the purposes of serving you more relevant ads about our Services. Where we provide you with interest-based ads on a site other than our own, we do not track your other activities on that site. If you click on our ads, we will know the domain you came from. For more information, please see the Cookies & Tracking Technologies section below.

Data from Third Parties

Third parties may provide us with personal data they have collected about you, from you, or from other online and offline sources. Marketing data from our partners and third parties can be combined with information we already have about you, to provide you with more relevant communications and to better tailor our offers to you. We make reasonable efforts to verify that the third parties we work with for marketing purposes are reputable, and we do not ask them to disclose your personal data if we do not have a lawful purpose and valid legal basis to collect and process that data.

Community Networking – NortonLifeLock Community (Forums, Blogs, and Networking Sites)

We operate forums, websites, and related information services, to better assist you in using our Services, discussing technical issues, and sharing your experiences. You should be aware that any data you provide in these public forums will be read, collected, and used by others who access them. To request removal of your personal data from any forum, contact us here. In certain circumstances, we may not be able to remove your personal data, in which case we will let you know why. Please note that your use of these community services may be subject to additional terms and conditions.

How to Opt Out of Interest-Based Advertising

We partner with third parties to display advertising on our website or to manage our advertising on other sites. You may opt out of many third-party ad networks, including those operated by members of the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA). For more information and available choices for third-party ad networks participating in the NAI and DAA programs, please visit their respective websites: www.networkadvertising.org/optout_nonppii.asp (NAI) and www.aboutads.info/choices (DAA). If you are in the European Union, you may also do so by visiting Your Online Choices (click here). Please note that if you opt out, you will continue to receive generic ads not based on your interests. Opting out of these networks does not otherwise limit the collection of information described elsewhere in this Statement.

Note: If your browser is configured to reject cookies when you visit the opt-out page, or you subsequently erase your cookies, use a different computer, or change web browsers, your opt-out may no longer be effective.

Cookies & Tracking Technologies

Cookies

A cookie is a commonly used automated data collection tool. Cookies are small text files that are placed on your computer or device by websites that you visit or HTML-formatted emails you open, to make websites work, or work more efficiently. We and our partners use cookies and other similar tracking technologies such as Web Beacons, JavaScript, clear GIFs, pixel tags, HTML5, and Flash Local Storage Objects on our websites or emails to:

- Enable the proper functioning of our websites and the proper delivery of legitimate electronic communications;
- Tailor information presented to you based on your browsing preferences, such as language and geographical region;
- Collect statistics regarding your website usage;

...
• Provide us with business and marketing information; and
• In some cases, to enable a third party to deliver future advertising for our Services to you when you visit certain websites owned by third parties.

We use different kinds of cookies:

• **Essential cookies** are necessary to provide you with Services and features available through our websites. Without these cookies, services you may need, such as shopping carts or e-billing, cannot be provided.

• **Advertising cookies and tracking scripts** are used to make advertising messages more relevant to you. They perform functions like preventing the same ad from continuously reappearing, ensuring that ads are properly delivered and, in some cases, featuring ads based on your interests.

• **Social Media cookies** collect data regarding social media interactions.

• **Analytics cookies** collect data that is either used in aggregate form to help us understand how the website is being used or to understand the effectiveness of our marketing campaigns.

• **Performance and Functionality cookies** collect data that is used to help make the user experience better on our websites.

The cookies we use include “session” cookies that are erased when you leave our websites, or they may be “persistent” cookies that remain on your computer’s hard drive after you leave the site, in preparation for your next visit to our websites.

If you do not wish to receive cookies, you may be able to refuse them by not agreeing to the use of them upon entering the website. If you do so, we may be unable to offer you some of our functionalities, Services, or support. If you have previously visited our websites, you may also have to delete any existing cookies from your browser. If you would like to view or manage the cookies we use, please see our cookie banner which is displayed when you first access our website, or the “privacy settings” tab located on the lower right hand of our websites.

**Third-Party Data Collection**

Cookies may also be placed on our websites by third parties to deliver tailored information and content that may be of interest to you, such as promotions or offerings, when you visit third-party websites after you have left ours. We do not permit these third parties to collect personal data about you on our sites beyond such cookies (e.g., email address) unless such data is provided to the third party in their role as a service provider acting solely on our behalf.

**Social Media Features and Widgets**

Our websites include social media features, such as Facebook’s “Like” button, and widgets, such as the “Share This” button, or interactive mini-programs that run on our sites. These features are usually recognizable by their third-party brand or logo and may collect your IP address or other personal data, including which page you are visiting on our websites, and set a cookie to enable the feature to work properly. Any collection of information through such third-party feature is governed by the privacy policy of the company providing it.

**Do-Not-Track Signals and Similar Mechanisms.**

Some mobile and web browsers transmit “do-not-track” signals. Because of differences in how web browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they are even aware of them. We currently do not respond to these signals.
Automated Individual Decision-Making and Profiling
Where NortonLifeLock processes network traffic data for the purpose of network and information security based on our or our customers’ legitimate interest as outlined in the corresponding section of this Statement, automated decisions concerning data elements may occasionally be made. This could involve assigning relative cybersecurity reputation scores to IP addresses and URLs based on objective cyber-threat indicators measured by our and our partners’ cyber-threat detection engines. Such indicators may be, for instance, the determination that malicious or otherwise harmful contents are hosted at a given URL or are coming from a given IP address. Such automatically assigned reputation scores may be leveraged by you, by NortonLifeLock, by our partners, and by other customers to detect, block, and mitigate the identified cyber threats. They could therefore result in our Services blocking network traffic coming from or going to such URLs and IP addresses. This processing is intended only to protect you, NortonLifeLock, our partners, and our other customers from cyber threats. If you consider that such automated processing is unduly affecting you in a significant way, please contact us as explained above (“Contact Us”) to raise your concerns and to seek our help in finding a satisfactory solution.

Children’s Privacy
Our websites are not directed to, nor do we knowingly collect data from, minors (as defined by applicable law) except where explicitly described otherwise in the privacy notices of Services designed specifically for purposes such as to assist you by providing child online protection features. In such cases, we will only collect, and process personal data related to any child under 13 years of age that you choose to disclose to us or otherwise instruct us to collect and process. Please refer to the Product Specific Privacy Statements for additional information.

Changes to this Statement
We reserve the right to revise or modify this Statement. In addition, we may update this Privacy Statement to reflect changes to our data practices. If we make any material changes in the way we collect, process, and/or share your personal data, we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. In the case of a material change to our personal data processing practices, any such change will only apply on a going-forward basis. We will not process the personal data currently in our possession in a materially different way without your prior consent. We encourage you to periodically review this page for the latest information on our privacy practices.

Links to Other Websites
Our websites may contain links to other websites owned or operated by other companies. If you visit any linked websites, please review their privacy statements carefully. We are not responsible for the content or privacy practices of websites that are owned by those third parties. Our websites may also link to co-branded websites that are maintained by NortonLifeLock and one or more of our business partners who are collecting your personal data pursuant to their own privacy practices. Please review the applicable privacy statements on any co-branded site you visit, as they may differ from ours.

Disclaimer
This Privacy Statement does not apply to NortonLifeLock affiliates: (1) Avira Operations GmbH & Co. KG., including its related entities; and (2) BullGuard Limited, including its related entities. These entities maintain separate privacy statements which can be found on their respective websites.

EFFECTIVE DATE: March 1, 2021