Explanation for approach:
My goal as a technical writer is to communicate clearly, accurately and concisely. Therefore my intention for rewriting the article was to maximize clarity while minimizing the number words. Where I felt there was redundancy, I eliminated words and/or combined sentences.

Rewritten article:

End-to-end encryption

Privacy and security is in our DNA, which is why XXX is built with end-to-end encryption. That means your messages, photos, videos, voice messages, documents, status updates and calls are secure.

Personal Messaging
End-to-end encryption ensures only you and the other user, and not even XXX, can read or listen to your messages. End-to-end encrypted messages are automatically secured with a lock, and and only you and the other user have the key.

Business Messaging
All sent and stored messages on the XXX Business app are end-to-end encrypted using the Signal encryption protocol before they leave your device. That means your messages are delivered securely.

However, messages are subject to a business's privacy practices. The business may designate other employees, or even vendors, to process messages.

Some businesses choose XXX's parent company, Facebook, to securely store and respond to customer messages. While the ads you see are not automatically informed by your messages, businesses may use chats for their own marketing purposes, which may include Facebook advertising. You can contact businesses to learn their privacy policies.

Note: The status of end-to-end encrypted chats can't change without being visible to the user. You can learn more in this white paper.

Payments
Payments in XXX, available in select countries, enable transfers between financial accounts. Card and bank numbers are stored encrypted in a highly-secured network. However, financial institutions can't process transactions without payments-related information, so these payments are not end-to-end encrypted.

"Verify Security Code"
End-to-end encrypted chats have a unique security code.This code can be found in the contact info screen, both as a QR code and a 60-digit number.

The actual key is always kept secret. Codes are unique to each chat and can be verified by both parties.

Note: Verification is optional.

To verify:

1. Open the chat.
2. Tap on the contact.
3. Tap Encryption to view the QR code and 60-digit number.

    - **Note**: Only available for contacts in end-to-end encrypted chats.

Two people in the same location can scan each other's QR code or visually compare the 60-digit number. When a QR code is scanned, a green check mark will appear confirming the codes match and messages are secure.

If the codes don't match, or your contact has recently reinstalled XXX or changed phones, refresh the code by sending a new message and then scaning the code again. You can learn more in this article.

If physically separate, you can send your contact the 60-digit number, which they will verify in the contact info screen under Encryption. For Android and iPhone, the Share button can be accessed from the Verify Security Code screen.

What does end-to-end encryption mean for keeping people safe?
Security is essential to XXX. We've seen multiple examples where hackers illegally obtained private data and abused technology to harm people.

Encryption and decryption happens on your device, so XXX cannot see messages or listen to calls. Messages are secured with a cryptographic lock that changes with every message, and only the recipient has the keys. You can find more details in this white paper.

What does this mean for law enforcement? XXX appreciates the work of law enforcement agencies. We carefully review, validate and respond to law enforcement requests based on applicable law and policy while prioritizing emergency requests. You can read more here.

To learn more about XXX's security, please visit WhatsApp Security.